WORD COUNT: 13056 LINE COUNT: 01067

9/3/6 (Item 3 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

04812991 SUPPLIER NUMBER: 09408681 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Employee dishonesty and workplace security: precautions about prevention.
103
Kandel, William L.
Employee Relations Law Journal, 16, n2, 217-231
Autumn, 1990
ISSN: 0098-8898 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 6632 LINE COUNT: 00561

9/3/7 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01319939 SUPPLIER NUMBER: 08042740 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Does your DP department bear investigation? (data processing)
103
Finn, Tony
DEC User, p56(2)
Dec, 1989
ISSN: 0263-6530 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 2187 LINE COUNT: 00159

9/3/8 (Item 1 from file: 553)
DIALOG(R)File 553:Wilson Bus. Abs. FullText

02826626 H.W. WILSON RECORD NUMBER: BWBA94076626 (USE FORMAT 7 FOR FULLTEXT)
You're a what? Data security analyst.
103
AUGMENTED TITLE: Fannie Mae's J. Jeffers
Mariani, Matthew
Occupational Outlook Quarterly (Occup Outlook Q) v. 38 (Summer '94) p. 39-41
LANGUAGE: English
WORD COUNT: 1907

9/3/9 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

203
02713693 Supplier Number: 45505497 (USE FORMAT 7 FOR FULLTEXT)
Network security
Computer Fraud & Security Bulletin, pN/A
May, 1995
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 436
?

ykk2_5W02_gbfaptr

thrown out with the rest of the rubbish?

No auditor likes to see a tape or disc labelled 'Meglamania Ltd Profit & Loss Report, Q2 1989' hanging out of a bin bag outside the back door of the building, even if the media has been demagnetised. It pays to make periodic checks that media and confidential data are being disposed of correctly. It is also worth considering the employment of a confidential waste disposal company to remove your secure rubbish and dispose of it properly.

Another area to be investigated is the disposal of printed output by user departments. It is a fact of life that a percentage of all printed output is filed under WPB (waste paper bin) without ever being read by the recipient. A further percentage of reports is dumped within a week of receipt and only a small percentage is filed away for reference purposes. This means that a large amount of the company's data is dumped in bins along with Mars bar wrappers and empty cigarette packets, while it is still current, providing the competition with untold opportunities to access this data and use it to build up a picture of the company's activities.

This may sound a bit fanciful, but before you dismiss the possibility, consider the fact that in the UK today there is a fast growing market in electronic surveillance and electronic eavesdropping equipment. If people are prepared to use these devices to spy on the competition, how do you know that your competitor doesn't pay one of your office cleaners to collect reports every day and pass them on?

Once again the use of a confidential waste disposal company will reduce the risk of secure waste falling into the wrong hands. It is sensible to place special secure waste bins in each department and to encourage the department managers to use this method to dispose of confidential reports.

Microfiche has grown in popularity for storing reports, and the disposal of microfiche needs to be looked at carefully along with the disposal of printed reports. Disposal via a confidential waste disposal company would again appear to be the safest route.

Many people would argue that the security and disposal of old magnetic media, reports and microfiche is the responsibility of office services, and not the IT department. I would suggest that it's a joint responsibility, especially when one considers that IT staff know better than most how sensitive the information on the media or in the reports is.

It may also seem poetic licence to deal with these items under the heading 'physical access security', but surely the act of taking away media or printed reports is 'physical' access?

If your site already has adequate procedures to deal with the problems outlined so far, the chances are that your auditor loves coming to your site, and for you God is in His heaven and all is right with the world. For most of us, this state of Nirvana is always aimed for but never achieved. Don't despair -- at least, not yet.

BACKUP STORAGE. Most sites make regular backups of their disc storage, but not all sites put the backups off-site. For our purposes, off-site means in a different building to the primary storage media, not necessarily 50 miles away in a bomb-proof bunker.

Many users feel that it is sufficient to put the backup tapes in a fire-proof safe in a corner of the computer room to give all the protection they need. I will relate a cautionary tale especially for these people and let them draw their own conclusions.

Some years ago, a businessman in Belfast decided to invest in a fire-proof safe for his backup tapes. He purchased a quality safe with all the latest features, and installed it in the corner of his computer room on the third floor of his building. One night, a car bomb went off outside the building, and the building was badly damaged by fire as well as by the impact of the blast. The next morning, the businessman was shocked to see the extent of the damage, but offered a silent prayer of thanks that he had invested in a fire-proof safe.

However, the police refused to allow him access to the safe, which had fallen from the third to the ground floor but was still intact, because the whole building was unstable. By the time the building was stable enough for the businessman to be allowed near his safe, five days had passed and

he had gone out of business. When he opened the safe, all the tapes were in good condition, and had survived the safe's fall as well as the explosion and the fire.

A number of specialist 'storage firms will collect your off-site storage material from your site and store it in a controlled air-conditioned environment for you. Typically they will deliver it back to you within an agreed time, any time, day or night. For this level of peace of mind, you will pay a fee.

Those of you who don't need this type of service can consider a reciprocal arrangement with another user, or can store the backup media at another of your company's offices, or you can put the backup media in the vault of your local bank. In short, there are any number of means available to you to satisfy your off-site storage requirements. The important point is that you realise that a fire-proof safe on its own is not enough to **protect** your corporate **data** , and that is what your auditor will be concerned with.

DESCRIPTORS: Data Processing; Auditing of Computer Systems; Data Security ; Tutorial
FILE SEGMENT: CD File 275
?

? t s9/3/all

9/3/1 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/INFORM(R)

01564048 02-15037
Data protection : **In pursuit of information some background to, and implementations of,** data protection **in Finland**
Saarenpaa, Ahti
International Review of Law, Computers & Technology v11n1 PP: 47-64 Mar 1997
ISSN: 1360-0869 JRNL CODE: IRLC
WORD COUNT: 10610

9/3/2 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/INFORM(R)

01413855 00064842
Intellectual property rights in data?
Reichman, J H; Samuelson, Pamela
Vanderbilt Law Review v50n1 PP: 49-166 Jan 1997
ISSN: 0042-2533 JRNL CODE: AVLR
WORD COUNT: 56562

9/3/3 (Item 3 from file: 15)
DIALOG(R)File 15:ABI/INFORM(R)

01208644 98-58039
Legal lessons in the computer age
Rasch, Mark D
Security Management v40n4 PP: 59-67 Apr 1996
ISSN: 0145-9406 JRNL CODE: SEM
WORD COUNT: 4545

9/3/4 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

08844434 SUPPLIER NUMBER: 18335123 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Legal lessons in the computer age.
Rasch, Mark D.
Security Management, v40, n4, p59(6)
April, 1996
ISSN: 0145-9406 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 4840 LINE COUNT: 00400

9/3/5 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

06806645 SUPPLIER NUMBER: 14886954 (USE FORMAT 7 OR 9 FOR FULL TEXT)
The EC proposed data protection **act.**
Mei, Peter
Law and Policy in International Business, 25, n1, 305-334
Fall, 1993
ISSN: 0023-9208 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT

? *t s9/full/1*

9/9/1 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/INFORM(R)

01564048 02-15037
Data protection : **In pursuit of information so**
implementations of, data protection **in Finland**
Saarenpaa, Ahti
International Review of Law, Computers & Technology
1997 ISSN: 1360-0869 JRNL CODE: IRLC
DOC TYPE: Journal article LANGUAGE: English LENGT
SPECIAL FEATURE: References
WORD COUNT: 10610

just after a/w.

ABSTRACT: The principle of publicity and access t
very topical issues in the European Union. For Fi
principle of publicity, in particular, has produce
for the rest of Europe has just begun debating
established a long time ago.

TEXT: From Publicity to Privacy

The principle of publicity and access to public information are very topical issues in the European Union. Publicity, as the right to obtain information from the **authorities** , is gradually being increased-or so it seems-and for a number of years now we have seen a spirited debate on public information. For Finland, discussion of the principle of publicity, in particular, has produced smiles of satisfaction, if not outright smugness, for the rest of Europe has just begun debating a principle that we have had for a long time! Finland is unquestionably one of the pioneers of right of access to public information in Europe, a fact often forgotten when Sweden is lauded as the premier example of right of access legislation. While it is true that Sweden enacted what is considered the world's first right of access law, its Freedom of the Press Act of 1766, it is equally true that Finland was part of the Kingdom of Sweden at that time. In other words, the Finnish principle of publicity is just as old as the Swedish. The honour of being the first country to adopt the principle is thus a draw between two Nordic countries.

It is interesting and significant to observe that on the national level Sweden was every bit as much a pioneer when the era of **data protection** legislation dawned, bringing its **Data Protection** Act (datalagen) into force back in 1973. Privacy and publicity were implemented legislatively at the same time in the homeland of right of access, and this, if anything, is a telling example of how a strong right-of-access principle can exist alongside a robust, modern concern for privacy in the form of **data protection** . What at first sight might seem to be strongly contrary principles need not be mutually exclusive in a democratic constitutional state.

The national bond between Finland and Sweden has long since ended (the early 1800s), but very strong parallels in legislation endure between the two countries. On a broader level, we can speak of a Nordic family resemblance among the bodies of legislation in many branches of law-especially private law. Thus, on balance, it was only natural that Finland followed Sweden's example very early on when the need arose to regulate **data protection** . When the Swedish **data protection** legislation came into force, a committee chosen on political grounds was busy drafting a **data protection** law in Finland, the expectation being that Finland would follow Sweden's lead with a delay of several years. This was not to be the case, however. Permit me to cite a passage from a recent

article of mine to summarize the relevant events:

The law-making process and the legislative history of **data protection** in Finland are short but colorful. Internationally, Finland was active early on, taking its first official step in drafting **data protection** legislation back in 1971. The bases for the new legislation were sought from neighboring Sweden-as was usual, especially in the field of private law-but after two years the work was discontinued; the Government had to abolish the committee which had been drafting the **data protection** legislation.1 The main reason for what in Finland was a very exceptional development lay in the strong tension between two different legislative and political attitudes, i.e. views on the Left emphasizing the social significance, power and inconvenience of different data systems in society, and on the Right advocating extensive freedom to collect and use personal information.2 No political compromise was achieved in the basic drafting work. Political parties and labor market organizations could not look forward-or even backward. **Data protection** was simply too new an issue to be assessed perspicaciously in the tense political climate of the time.

When active drafting work resumed towards the end of the 1980s, we were, from the international point of view, already in the midst of a new phase in the development of **data protection** legislation. The final touches were being put on the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, marking the emergence of the first common principles of **data protection** in Europe. At the same time, the rapid development of information technology in society was changing the way we work daily, a trend affecting in particular office automation and the collection of information related to it. Developments which the legislators of the 1970s could only project were already plainly observable in society. These changes, and, of course, the experiences which different countries had already gained in the field of **data protection** , figured in the bill brought before Parliament by the Finnish government in 1986.3 The bill contained the draft of an act-the Personal Data File Act-which can well be characterized as a second-generation **data protection** act. Dallying on the road paved by Sweden actually proved advantageous for Finland, although, with the Act not coming into force until 1988, the country clearly fell behind the front runners in the field internationally.

Space does not permit me to deal with the Personal Data File Act in its entirety, so I will content myself to list the following salient technical legal solutions adopted in the legislation:

The Personal Data File Act is a secondary general law.

The Personal Data File Act only applies to the data of natural, non-public persons, not to the data of corporations and companies.

The Personal Data File Act is a law for monitoring the life cycle of personal data.

The Personal Data File Act distinguishes between the use of the data by the controller of the personal data file for operational purposes and the transfer of the data to an outside party.

The Personal Data File Act is legislation predicated as a rule on the self-control- **without permission** -of the controller of a personal data file.

The Personal Data File Act is a law of flexible definitions. According to the Personal Data File Act, data subjects ordinarily have a right to check what information on them has been entered into the personal data file.

8 The Personal Data File Act is a law containing instructions for internal

interpretation.

9 The implementation of the Personal Data File Act in practice is entrusted to the special **data protection authorities** .

10 The Personal Data File Act is a law containing an extensive system of exceptional permits by the **data protection** board.4

A personal data file act in a country where publicity has reigned supreme is a difficult issue, especially for those who are accustomed to exploiting the principle of right of access and the access it guarantees. As Kauko Wikstrom has put it, every new law that comes into force opens a field of possibilities.5 It takes time for interpretations to become established in practice; and when a new principle emerges alongside a traditional one, and is contrary to the old, the time required for it to become established may be long indeed. This has certainly been the case in Finland. The relation between the principle of publicity and the principle of privacy is still not a stable one. Where interpretation is concerned, the situation is-to quote Wikstrom again-wide open.6 One significant change has taken place, however: the system of fundamental constitutional rights in Finland was reformed in 1995, and both **data protection** and the principle of publicity are now inscribed in the constitution. **Data protection** is provided for in section 8.1, which concerns private life, honour and domestic peace, whereas the principle of publicity is covered in section 10, which deals with freedom of speech. It will be worthwhile to present the relevant provisions of each section:

8.1: The private life, honour and home of every person shall be secured. More detailed provisions on the **protection** of personal **data** shall be prescribed by Act of Parliament. 10.2: The documents and other records in the possession of public **authorities** shall be public unless their publicity has been separately restricted by Act of Parliament for compelling reasons. Everyone shall have the right to obtain information from public documents and records.

The manner in which **data protection** is presented in the Constitution is perhaps not entirely successful. Those of us who appreciate **data protection** as an integral part of the protection of privacy would have preferred more extensive treatment of the matter. In any event, the obligation to prescribe more detailed provisions on **data protection** by Act of Parliament means in practice that **data protection** has the same constitutional status as the principle of publicity. Together, the provisions prove that privacy and publicity are principles of equal rank which comprise part of our fundamental rights and which must be implemented on the level of law as an Act of Parliament. As far as interpretation is concerned, the situation should no longer be wide open, or, indeed, even relatively open.7

The second-generation **data protection** act will be followed by a third-generation act in 1998 at the latest. The EU Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such datas will require Finland, too, one of the more recent member states, to implement its **data protection** legislation in accordance with the terms of the Directive.9 The Directive specifies, and in fact significantly changes, some procedures adopted by the Council of Europe **Data Protection** Convention, and, all in all, seems to protect privacy better than the latter. This fact alone permits us to describe the Directive as a third-generation piece of legislation. Other **data protection** directives-for example, in telecommunications-by the EU will also embrace the same trend. The regulation being implemented on the directive level thus goes into more detail than a mere general **data protection** directive would provide.

We have not, however, completed the transition from publicity to privacy,

nor are we even on the way. While the manifest adoption of the principle of publicity as a panEuropean objective, like the new provisions of the Finnish constitution, does effect a type of balance between privacy and publicity, we must remain aware that in the worst case the Directive, despite its emphasis on **data protection** , may well be a step backwards. This claim may sound strange, for both the articles and recitals of the Directive resoundingly advocate **data protection** -but with one exception, point 72 of the recitals. This addition, insisted on by the Nordic countries-chiefly Sweden and Finland-reads as follows: 'Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive.' This seemingly minor addition at the end of the recitals is interesting in a number of ways. Among other things, it raises the issue of what recitals mean in practice and how one should read them. Can a statement such as that in point 72 really provide a means to circumvent the entire Directive? Questions like this have already been heard in Finland unofficially among advocates of the principle of public access, but we can probably dismiss such comments as being no more than what they are-unofficial statements. This example nevertheless drives home the point of just how difficult it is to read and interpret directives. It makes the above-mentioned amendments to the Finnish constitution particularly justified and timely from the point of view of **data protection** . The public and private domains are both important. On the way from public to private we stop, as seems fitting in the Nordic countries, at a reasoned balance between the two principles. It is only in this context that point 72 of the recitals in the **Data Protection** Directive makes any sense for the purposes of future legislation.

Data Protection as Respect for the Individual Citizen

Information is processed in many ways in the field of law. In reflecting on what information law might be, one readily observes that the law-maker employs a variety of legal constructions in the attempt to enact legislation on information. The route from copyright law to the various secrecy regulations is a long one.lo As a phenomenon, **data protection** is frequently associated with secrecy, above all in the view of its critics, who wish to give it a negative ring. The result is a bias of considerable proportions, for there is no doubt that some of the secrecy regulations serve the needs of society; they are regulations which, if abused, might even undermine the pivotal values of the constitutional state. Upon closer investigation, however, one notices that, as a rule, the secrecy regulations we have today have been drawn up to protect private persons. They are the rules by and for individuals which are needed to keep the constitutional state and the occasionally prying state distinct. The world in which a person's reputation was protected solely by libel regulations is simply no longer viable. In this perspective, most secrecy regulations are positive provisions embodying respect for the person and his/her privacy.

When the draft Personal Data File Act was brought before Parliament in April 1994, Christopher Taxell, Minister of Justice at the time, stated that the legislation was a law of respect for the person. He concluded his speech with the following words:

In my view, it is a vital element of Finnish society that people can trust in the pertinency of data file maintenance. Such activity cannot mean that a person and his/her private life fall totally under supervision of the **authorities** . We must respect the individual behind the personal identity number. Personal data file legislation is indispensable in the Information Society.

Despite its sound goals, the first years of **data protection** in Finland were somewhat **stormy** ones. The lofty notion of respect for the person remained largely the stuff of speeches. Although the pace at which the Act

was applied in practice was deliberately slow, genuine opposition to **data protection** appeared in many quarters, and was-after the discussions in Parliament-unexpectedly strong.11 I have perhaps overstated the differences on the issue of **data protection** , having spoken of its 'enemies' on occasion when a more appropriate term would be 'opponents of change'. Changes in familiar procedures naturally arouse resistance until the goals of the new ones have been internalized. And this is precisely what has happened on many fronts in the early years of **data protection** in Finland. The principle opponents of **data protection** and the reasons for their opposition are presented below.

The media, especially the press, took a negative view of **data protection** because the Act applied to the personal data files and archives they used and limited their opportunities to use public information freely.12
The bureaucracy in both the public and private sectors, because the Act limits the information content of databases and for the most part prevents the combination of personal data files.

Data-processing professionals, because unlimited use of the personal identity number, in particular, is restricted in the planning and implementation of information systems.

The police, because the Personal Data File Act restricts the combination of different personal data files and required special regulations for the data files maintained by the police. In certain situations, this hampered the supervision of persons and the investigation of crimes.

Direct marketing entrepreneurs, because the Act and its related decree significantly limited opportunities to collect and use information on persons for the purpose of direct marketing and other mass sales activities.

Scholars and historians, because research on persons must conform to strict rules on the collection and use of information. Moreover, the prescribed reduction in the content of personal data files and the obligation to erase unnecessary data files reduce the amount of material available to historians.

Editors of Who's Who and similar publications, because such publications, which are common, popular and profitable in the activities of different fields, educational institutions and organizations, first required an exceptional permit from the **data protection authorities** .13

To my mind, these selected pockets of resistance-if that is the word-suffice to show how easily a basic tension arises between the flexibility sought in various activities and the requirements of **data protection** . In most cases, there is a bureaucratic tinge to this antagonism, although the bureaucracy proper is not involved. We want to deal with matters as simply as possible. However, this is one tendency which more generally threatens to undermine the procedures of the constitutional state and, consequently, people's fundamental rights. In fact, everyone who is put off by having to observe formal legal rules is also put off in one way or another by the nature of the constitutional legal state. The price that we pay in some individual cases-being ill at ease, to quote Georg Henrik von Wright-for the legal security of the constitutional state is very often respect for the person. No man is an island-at least not in our organized information society.
In the case of **data protection** , the issue is more than one of mere formal rules of law. By limiting the freedom to compile data files and to record data, we want to reduce the amount of that information on the average citizen which is freely available to others. Accordingly, **data protection** legislation has to be seen as an intertwining of formal and material law. It is a field in which rules of form cannot necessarily be distinguished from rules of content in the same way as they can be in

traditional legislation. In fact, this situation may in some cases either hamper or prevent us from discerning the objectives of the legislation. To overcome this potential handicap, the Finnish Personal Data File Act includes an internal interpretation guideline, mentioned above in connection with its technical-legal procedures. Section 3 of the Act, entitled 'the duty of care', reads as follows:

In collecting, recording, using and delivering personal data, the controller of the file shall take care and comply with good data file practice and also in other respects act so that the protection of the privacy, interests and rights of the data subject are not violated without cause and so that the security of the State is not endangered. A party who, as an independent entrepreneur or business, acts on behalf of the controller of the file or to whom the controller of the file has delivered personal data shall have the same obligation.14

This provision is interesting as a legislative technique, drawing, as it does, the attention of the interpreter of the Act to the purpose of the legislation. In fact the duty of care means a strong combination of material and procedural aims. The controller of a file must adhere to good data file practice in all his/her activities and promote both privacy and state security, although the latter is perhaps not so important today. The duty of care thus means something more important than an emphasis on the goals of the Act and the usual careful pursuit of those goals. The Act has its own internal guideline for interpretation, one going beyond the conventional doctrines of interpretation. What we really see here is an optimization order of sorts; the legislator did not want to leave room for the single interpreter's own value judgments. Good data file practice is merely an ideal, within the scope of which one must in practice respect the privacy of the data subject.

The importance of the duty of care is not easy to appreciate at first. The very term somehow fails to attract the lawyer's interest. One might imagine that the legislator is using the expression to refer to the care which lawyers are expected to exercise in their work anyway. Privacy, too, is a new legal term in Finland. As a matter of fact, Timo Konstari, the leading researcher on the principle of publicity in Finland, pointed out aptly in the early 1990s that privacy as a term is somehow vexing to those who must interpret the law.15 The situation today is quite different, however. The duty of care and the practical importance of good data file practice associated with it can hardly be overestimated in the **data protection** discussion nowadays. From the legislative point of view it is easy to see that as we approach good data file practice-a goal that most likely can never be achieved-the need for action by **data protection** officials will decrease and, accordingly, **data protection** will become established as one sector of good practice in society. When we have reached this situation, at some time in the future, **data protection** will have rid itself of the negative connotation it currently has in public discussion. For **data protection** officials this will also mean an opportunity to concentrate their efforts on solving so-called hard cases. And almost certainly there will never be a shortage of these.

It is interesting to observe that the European **Data Protection** Directive also takes respect for the person-the citizen-as its point of departure. This can been seen in the second point of the recitals:

Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansions and the well-being of persons.

We are thus in the process of enacting a third-generation **data protection** act on the very bases which Minister Christoffer Taxell articulated in the speech quoted earlier. **Data protection** is respect

for the person. This assertion now has-or should have-a broader, European sounding board.

When we speak of respect for the person, we are compelled to draw the line between privacy and publicity. In the process, two issues in particular emerge that require closer scrutiny in a constitutional democratic, legal state which seeks to uphold publicity. The first is the question of the relation between the legislation on **data protection** and that on right of access. The second is that of the possible differences between a person's public and private roles. The attempts that have been made in Finland to address these issues merit a closer look.

Privacy and Publicity

In reconciling privacy and publicity, one inevitably encounters technical difficulties in formulating the relevant legislation. How can we express the relation between **data protection** and publicity in the law? In answering this question, Finnish legislators in the 1980s adopted a restrained, almost invisible, attitude. The Personal Data File Act does not contain provisions which in a general form would in any way refer to the legislation on publicity. Nor does the Access to Public Documents Act include a corresponding general provision which refers to the Personal Data File Act. The two pieces of general legislation are thus not overtly linked to one another; nor, on the other hand, is it stipulated that they should be mutually exclusive.16 The only clear exception is section 18a of the Access to Public Documents Act, which contains the provision on mass delivery of public data.17 I will take up this topic below. First, however, it is necessary to examine on a more general level the lack of provisions which might prescribe the relation between the two statutes.

The basic point of departure in the solution adopted by the legislator is the status of the Personal Data File Act as a secondary general law. The debate on the different models for regulating **data protection** has included reflections on the need for a general law, a familiar concern internationally. Finland, essentially following Sweden's example, in fact ultimately opted for a general law, a decision that was intended to demonstrate the overall significance of **data protection** within one and the same law. It is easier to create a legal institutionwhich is in fact what **data protection** is-by enacting a general law than by implementing numerous special ones specific to individual fields. International development has very much proceeded in the direction of general laws.

The basic problem with a general law, however, is that it cannot-or can only unsatisfactorily-be applied in the regulation of special fields or issues. For this reason, the Personal Data File Act, too, is a general law, although a secondary general law. This status is apparent in section 1 on the applicability of the Act:

In order to protect the privacy, interests and rights of the person, to ensure the security of the State and to maintain good data file practice, the provisions of this Act shall be complied with, unless otherwise stipulated by law, in collecting, recording, using and delivering personal data.

By binding other legislation to the Personal Data File Act such that only Acts of Parliament (that is, not lower-level provisions) allow one to deviate from the Act, the legislator undoubtedly wanted to point out the importance of **data protection** . However, this solution only works well when other legislation has taken **data protection** into account, and this certainly was not the case when the Personal Data File Act came into force; nor is it true even today. This situation has made it difficult to recognize and interpret the relation between **data protection** and publicity of documents. The Access to Public Documents Act neither expressly provided for the same things as the Personal Data File Act nor

specified the matters it was intended to cover in as much detail as the latter. As a consequence, it was justifiable when examining provisions of the former to assume that public information as it related to personal data fell within the scope of both pieces of legislation. As a secondary general law, the Personal Data File Act applies to all situations which have not been provided for in a more detailed fashion elsewhere. The upshot of this situation in many cases was that many administrative **authorities** , invoking considerations of **data protection** , were unwilling to release personal data contained in public documents to citizens. The same rationale was extended to documents on the whole if they contained, as they almost always do, personal data. It is also possible that **data protection** has consciously been used in some instances as a tool to minimize right of access. Despite the principle of publicity, the significance of **data protection** seems to be overlooked in public administration. What is more, there seems to be a certain unwillingness to make matters under consideration available to the public, especially the press. **Data protection** has provided a suitable weapon against right of access.

The legislator's purpose was a totally different one, however. Although the publicity of documents had not yet been provided for in the Constitution, it was still considered a pillar of the Finnish constitutional state. The Access to Public Documents Act represented a special law in relation to the Personal Data File Act, whereby it became unthinkable to set aside considerations of the right of access when interpreting norms on **data protection** . This position can be found in the arguments in the Government bill, but these are not, in accordance with the Finnish doctrine of the sources of law, binding on those interpreting the law.ls This is what the legislators were thinking, but these ideas were not stated expressly in either act. The interpretation had to be derived from general doctrines. As most of the people working in public administration lack legal training, they would not find this task an easy one.

The relationship between the Access to Public Documents Act and the Personal Data File Act has reared its head visibly and somewhat embarrassingly for the Finnish judicial system. Invoking considerations of **data protection** , the Supreme Administrative Court, the only court of appeal in **data protection** matters, refused to release public information to a journalist who had requested it on the basis of the right-of-access legislation.19 The journalist referred the case to the Parliamentary Ombudsman. The essential details of the decision are contained in the following excerpt from a bulletin issued by the Ombudsman:20 The information officer of the Supreme Administrative Court had refused to release to the journalist a computer-based internal record of the Court to be browsed at a computer terminal Moreover, the journalist was not allowed to read a hard copy of the record. The information officer justified his position by reference to section 18a of the Access to Public Documents Act, which prohibits mass transfer of personal data and thus browsing of the court record in question. In addition, the information officer mentioned that for technical reasons the secret and public data in the record could not be separated.

The computerized record of the Supreme Administrative Court is a personal data file in the sense of the Personal Data File Act. In interpreting the concept of mass transfer, the essential issue is whether in browsing the record the user intended to collect and record large amounts of personal data with a view to forming a new data file. According to section 7, paragraph 2 of the Access to Public Documents Act, mere browsing of the record in order to obtain public information from the **authorities** cannot be construed as mass transfer as defined in the Personal Data File Act.

Right of access to the record should be arranged such that users can obtain the data they wish in the alternative ways prescribed in section 7, paragraph 2 of the Access to Public Documents Act, on the condition that these data are not secret, non-public or classifiable as a sensitive sample

for the purposes of browsing in the sense of the Personal Data File Act. This requires, however, that the public information in the record has been defined and that the contents of the file which are other than public can be easily separated by technical means. In order for browsing to be possible at the terminal, the browsing software should be capable of preventing the compilation of a sensitive sample.

It is my understanding that the plaintiff should have been granted the right to browse a hard copy of the record containing the public entries therein.

It is proposed that the Supreme Administrative Court should undertake measures to organize its internal record such that it is technically possible to separate the information therein which has been defined as public.

When the legislation on **data protection** came into force, it showed how muddled the legal status of the internal administrative records maintained by different **authorities** was. What had always been considered technical tools in office data management had become data files, and, in most cases, personal data files in the sense of the Personal Data File Act. The significance of different records as data **stores** was previously vague. Yet the situation described above involving the use of an internal court record is an everyday one in information retrieval for both the media and private citizens. It was only a matter of time as to where and how an apparent problem would come up in applying the legislation to cases at the interface between the two acts. It is paradoxical indeed that a misconception concerning the status of the two acts vis-a-vis one another should occur in the Supreme Administrative Court.21

The conclusion of the Parliamentary Ombudsman in the case is indisputably correct. **Data protection** cannot supersede the right of access to public information. The rationale for his decision seems seriously flawed, however. The notion that browsing a record does not constitute mass delivery is clearly at variance with section 2 of the Personal Data File Act and the related preparatory documents:

'mass delivery' means the delivery of all the personal data in the personal data file or of data concerning a relatively large number of data subjects recorded in the file as well as the delivery of personal data in a form suitable for automatic data processing or so that the party to which the data are delivered can use the personal data file by utilizing a technical connection.
Browsing of the data file using a technical connection amounts to mass delivery in the light of this definition, regardless of whether one is searching for an individual piece or a larger body of data. The crucial circumstance is that the data store is available in its entirety to the person retrieving data. Browsing a court record at a terminal is in itself to be construed automatically as mass delivery as defined in section 2 of the Personal Data File Act. As the right of a citizen to obtain information on individual cases provided for in section 7 of the Access to Public Documents Act cannot not be exercised owing to the prohibition on mass delivery set out in section 18a of the Personal Data File Act, we find ourselves faced with the interesting situation regarding to interpretation suggested above. The definition of mass delivery precludes the exercise of the principle of right of access intended in the Act. The natural interpretation of this situation is that the Personal Data File Act should yield to the express special provision in the Access to Public Documents Act; a conflict of laws is resolved in favour of a special law. But this was overlooked in the decision of the Parliamentary Ombudsman. In other words, the problem was not identified correctly in the legal sense.

When two significant bodies entrusted with interpreting the law, i.e. the Supreme Administrative Court and the Parliamentary Ombudsman, experience

difficulties with fundamental questions of interpretation, we can hardly say that the legislators have chosen a successful approach. On the other hand, it is difficult to manage this situation legislatively, because the browsing of an internal administrative record most certainly falls under the principle of right of access. A citizen cannot be required to have a detailed knowledge of a matter which he/she is trying to clarify. This is one difficulty that must be addressed in future legislation.22

The legislation on the right of access in Finland is currently being reformed, and certain additional provisions to the Act have been proposed which would clarify the relation between publicity and privacy. It is evident that such are needed. Yet it is every bit as important to inscribe a distinct position in the **data protection** legislation on how the legislation should be applied in conjunction with the legislation on the right of access. It is only when we have references in both directions that a regulatory model can be found which, in view of the equal status of the statutes, sufficiently helps the people who apply the laws.

What is more, since the principle of publicity on a broader scale is establishing itself throughout Europe, similar procedures will have to adopted elsewhere as well. The informative content of legislation should be of a high standard. The principle of publicity and public information should not invite a deviation from the straight and narrow path of **data protection** . It seems to me that this issue was not considered carefully enough when the European **Data Protection** Directive was being drafted. The matter would have to be addressed even without point 72 of the recitals. The Council of Europe Convention should have obligated member states to examine the boundary between privacy and publicity from the standpoint of legislative techniques. It is hardly an exaggeration to assume that the next few years will spawn a range of interpretation problems, especially with the media looking for the boundary between what is permitted and what is prohibited in the legislative jungle of privacy and publicity.

The Private and Public Person

The distinction between private and public has cropped up-and continues to do so-in considerations of the privacy of public figures. In fact, this has been one of the fundamental issues in the legal debate on privacy ever since the discipline of law took an interest in the subject. The question has many different dimensions, ranging from using the picture and name of a well-known artist to revealing the private life of a politician. The publicity of official information contributes a dimension of its own.

In Finland these issues were dealt with for a long time in the context of the provisions on libel and slander. In other words, the point of departure was that mainly false information had been given about a person. As the 'yellow press' did not have a wide circulation in Finland until the 1960s, the debate on the relation between freedom of the press and privacy, familiar in many countries, was quite late in getting started. In response to a number of articles, one of which actually resulted in the suicide of an artist, efforts were mounted in the early 1970s to draft legislative measures to address the issue. The outcome of this work by the Commission on Freedom of the Press was the so-called protection of privacy provision.23 A new paragraph (Criminal Code 27(3a)) was added to the provisions of the Criminal Code on libel in 1974:

A person who unlawfully through the use of the mass media or in another similar manner publicly spreads information, an insinuation or an image of the private life of another person, conducive to causing him damage or suffering, shall be sentenced for invasion of privacy to imprisonment for at most two years or to a fine. Publication that deals with a person's behaviour in public office or in a public duty, in professional life, political activity or in other comparable activity, when this is necessary

in dealing with a socially important matter, shall not be considered invasion of privacy.
As the text of the provision indicates, the issue is no longer one of spreading wrong information. The transition from libel in the traditional sense to a genuine protection of privacy has taken place. Spreading true information unlawfully is also a punishable offence. The above provision provides rather good protection for the average citizen. In contrast, a public person, e.g. a civil servant, politician or businessman, is in a weaker position. The boundaries of their private lives are defined only upon a consideration of interests. A matter of great societal significance can supersede considerations of the protection of privacy, making the provision a culturally bound discretionary rule of law.

In Finnish society, the past few decades have been a time of public disclosures; that is, the privacy of figures in the public eye has been poorly protected. Even on the relatively rare occasions when politicians or civil servants have reported alleged invasions of privacy, the public prosecutor has generally failed to press charges. Perhaps the most revealing example of this trend is an incident that occurred in the early 1980s. A fight arose between two women visiting the President's adjutant, the altercation taking place in the adjutant's official residence, which is located in the same complex as the President's. The press gave the case extensive and visible coverage, boosting sales with full details of the adjutant's name and duties. The adjutant, who ultimately resigned because of the incident, invoked protection of privacy-but in vain; the public prosecutor refused to press charges. I bring this case up time and time again in my courses as an example of just how poor the protection of privacy for a public person can be despite the existence of a provision on the right.

However, when **data protection** legislation was being drafted, it was the very protection of privacy provision in the Criminal Code that served as an example of how and where to draw the line between the public and private domains. In the Personal Data File Act, the same distinction has been observed by limiting the Act to apply to private, natural persons. The Personal Data File Act only applies to the data of natural, non-public persons, not to the data of corporations and companies. This can be seen in the following definition in section 2 of the Act:

For the purposes of this Act:

1) 'Personal data' means a description of a person or a person's characteristics or living circumstances which can be recognized as depicting a certain natural private person or his family or those living with him in the same household.
The distinction between private and public persons has caused, and will continue to cause, numerous problems in **data protection** practice. The question is no longer one of what is published but of what information may be collected, used and supplied to other parties. This being the case, we should have some idea of the data which belong to the private domain to begin with; but we do not. A demarcation of sorts between the two domains for other situations can be found in the Personal Data File Decree, which defines the basic permissible content of publications such as Who's Who. These may contain a person's name and his/her spouse's name, date and place of birth, date of marriage, time and place of death, title and profession as well as his/her children's and parents' name, date and place of birth, time and place of death, title and profession. Although a person may currently have the right to forbid the use of personal data in a Who's Who publication, the above list indicates the legislator's notion of the basic bounds of privacy. By including a person's wedding day and his/her children's dates of birth in the standard information that can be printed in such publications, the statute makes plain the idea that it is a public, rather than a private, matter whether a family has children conceived or born before the parents were married. In this respect, the legislation can hardly be said to reflect the current values in Nordic society, or in many

others for that matter. The example also shows just how culture-bound issues of **data protection** are in the final analysis.
It will be instructive here to mention briefly the most recent highly publicized case in Finland involving the privacy of public persons and causing problems in the interpretation of the legislation. In October 1996, on the day on which both municipal and EU parliamentary elections were being held, Helsingin Sanomat, the country's largest newspaper, asked the Ministry of Justice for data on the ages of the candidates. The ministry refused to release this information, referring to the Electoral Act, the provisions of which state that it is not permitted to disclose a person's personal identity number. In Finland this number includes a person's date of birth.24

However, in the present case, the press found out this information through other sources, that is the population register provided them with the data they wanted. The law did not prevent this, although the population register cannot disclose a person's full personal identity number either. This example demonstrates plainly how difficult information management can become if the relevant legislation is not coordinated properly. The main issue itself is fairly straightforward. The age of a candidate standing for election is a public matter at the time of elections. Voters must have the right to know the age of the person or persons they are voting for. In contrast, a candidate's date of birth is a private matter.
We are again faced with drawing the line between public and private persons when, as in the case above, we try to determine who is a public person and who is a private one. The Personal Data File Act does not provide a detailed definition. Only the general rule of interpretation in section 3 of the Act guides us unswervingly towards a strict interpretation: in cases of uncertainty, it is justified in light of the Act to infer that a person's privacy must be protected. This situation is most apparent when the controller of the file and the person invoking right of access differ in their views on the matter. The Act does not include any procedures for such contingencies, and this is doubtless a shortcoming as far as transfer of data is concerned.25

In Finnish **data protection** practice, we have already encountered cases in which personal data suddenly become public owing to a lack of regulation through special legislation. The Supreme Administrative Court has accepted an interpretation whereby the data in the Trade Register on persons engaged in business (even on a very modest scale) or in business management relate to the public position of these persons and thereby may be freely delivered to third parties, even for commercial purposes. This interpretation is, in my view, contrary to the guideline in section 3 of the Personal Data File Act.26
The European **Data Protection** Directive contains no special regulations on the position of public persons. To be sure, Article 8, which deals with different categories of data processing, applies indirectly to politicians, for example, and its requirement of explicit consent by the data subject pertains to other public persons as well. Nevertheless, it seems that point 72 of the recitals, which favours the right of access to official documents, will ultimately continue to be the tool used in the Nordic countries to provide for the special position of public persons with regard to **data** .27 **Protection** of privacy for public persons, even if limited, is undoubtedly one of the building blocks of the legitimacy of the democratic constitutional state. We have, as Georg Henrik von Wright has expressed it, a need to know what is happening in the world around us.zs We must know how decisionmakers and influential people work, and addressing this need through legislative means is naturally a better solution than proceeding at the mercy of the many, often suspect, ways in which the media obtain their information.

Who Owns the Information?

In the previous sections, I have dealt with public information on both

private and public individuals as information which can be spread further if provisions do not stipulate otherwise. This is how we are accustomed to think, but we should ask whether this is the right approach. What entitles the **authorities** to sell information on us, information which they have generally collected by law-and by law only-from us? Do the **authorities** acquire title or a comparable right to our data?2

In Finland, the most prominent organizations where the sale of official information is concerned are the Population Register Centre and the Central Motor Vehicle Register Centre. The former maintains a system of census data on the entire population;3 the latter records information on all of the motor vehicles in the country. The legislation pertaining to both organizations is quite recent, having being introduced since the Personal Data File Act. The Population Data Act was implemented in 1993, the Road Traffic Communications System Act in 1989. The Personal Data File Act was thus on the books when each of these pieces of legislation was being enacted, and the data subjects in each act are given the opportunity to prohibit the delivery of their personal data to third parties for commercial purposes.31 The acts themselves have been implemented with a decided view to commercial use. In fact, section 3 of the Population Data Act mentions direct marketing as one of the potential purposes of the personal data recorded in the system. Likewise, the Road Traffic Communications System Act indicates that direct marketing is one purpose for which data may be delivered (section 11). These provisions show how public **authorities** work in two roles simultaneously. The citizen as an administrative subject is obliged to furnish data to officials, who maintain data files of importance to society and who, at the same time, exploit the file commercially. Our personal information is put to work to make money.

The European **Data Protection** Directive assigns a special status to information used for commercial purposes, especially direct marketing. Article 14 of the Directive stipulates that personal data can be used for direct marketing and other mass delivery only with the consent of the data subject. Accordingly, in the future, personal data will be divided into two categories: commercial and non-commercial information. Information will be earmarked for a particular purpose. This arrangement, if implemented effectively, will do much to improve the position of the individual citizen. We will have approached a situation in which citizens decide, within the bounds of their right of self-determination, how the information on them is used and distributed.

Despite the refinements provided by the Directive, it must be emphasized that the issue in **data protection** is not the ownership of data but the content and exercise of our right of self-determination. This particular fact is forgotten regrettably often in the international debate on the issue. In the Finnish legal literature, I have defined the right of selfdetermination as a concept in personality law which is based on our conception of the human being. The right can be further divided as follows:

the right to external freedom;

the right to internal freedom;

the right to competence;

the right to power.

In this breakdown the right to internal and external freedom is understood as a right of the individual to physical and mental immunity or inviolability. We also speak of integrity. The right to competence means primarily that in order to make free decisions a person should have sufficient discretion and information on the decision-making which affects and pertains to him/her. The fourth basic element of the right of

self-determination can be regarded as the right to make decisions concerning oneself and to have them carried out. We 'own' our bodies, thoughts and knowledge. This idea goes back as far as John Locke, who said that ultimately, in a way, people own themselves, too; and where they so desire they sell themselves.32 Today we can say that living as free citizens in a constitutional state presupposes the opportunity and the right to decide on the information concerning us and how this is used. Only the essential needs of society can provide justification for restricting a citizen's right of self-determination.

Data protection serves to realize our right to intellectual integrity, our right to competence and our right to power. It is thus one of the most important means we have of safeguarding our right of self-determination. It really is one of our freedoms.33 If we do not realize this, it will become impossible to discuss **data protection** rationally. If we merely debate the issue of who owns the information, our efforts will continue to fall wide of the mark. We would do well to speak of the right of self-determination and conscious domestic peace.

Data and Tantalos

Kaarle Makkonen has drawn a comparison in a brilliant fashion between norms and the fruits of Tantalos. Both are things we never attain. Legal text only gives us information on norms.34 **Data protection** legislation seems to be a body of legislation in which both the norms and their object-information-are like the fruits of Tantalos. The phenomenon and the events which are being regulated are so complex that comprehensive, unambiguous legislation seems impossible to achieve. We will constantly find ourselves in situations in which someone finds violations of **data protection** in everyday events or in which the existence of **data protection** is not acknowledged. Let me present two examples of this: In spring 1996, the Finnish **Data Protection** Ombudsman demanded that the **Data Protection** Board prohibit the economists' unemployment fund from sending letters to its members in envelopes which had the name of the fund on them. The person who reported this practice to the Ombudsman thought that having the name of the unemployment fund on the envelope would reveal an important piece of information about the recipient of the letter, i.e. that he/she is unemployed. The **Data Protection** Board did not approve the request. The issue was not considered to be one of **data protection** . Several years ago the Parliamentary Ombudsman took the position that job applications received by an employer did not constitute a personal data file because the employer had not defined the file in advance. The Supreme Administrative Court later adopted the opposing view. Failing to define a data file cannot prevent the application of **data protection** .35

Despite the difficulties involved, it is essential to enact laws providing for **data protection** . The crux of the matter is not the present obligations imposed by the Council of Europe Convention or the European Union Directive. The need for regulation lies on a deeper level, in our conception of the human being.

In the information society we are embarking on a transition to a constitutional state in which the fundamental rights of citizens figure more prominently than heretofore. If we content ourselves with **data protection** which rests on general principles or civil rights provisions of a general nature, it will be trodden underfoot by commercial interests. The legislative borderlines are, however, new. The price we pay for our increasingly complex **data protection** legislation is small compared to the spectre of having information become a mere factor of production detached from our right of self-determination. The law cannot keep abreast of developments in information exhaustively, but it can give us a better chance to protect our privacy. The present Finnish Personal Data File Act has, in my view, already borne this out sufficiently. However, we are still powerless against the worst enemy of privacy-the snooping neighbour.

Footnote:

Notes

I The societal significance associated with the regulation of **data protection** at that time can be seen in the fact that, even before the committee was set up, the Ministry of Justice had established a commission to deliberate the matter and had prepared the task for what was a clearly political committee.

2 The government's point of departure at that time can easily be seen in the name of the committee, which was called 'the Information System Committee'.

3 Although the bill clearly took the Council of Europe Convention into account, the latter agreement is not expressly mentioned in it. Moreover, the annexes to the bill give only a brief description of the Convention. The explanation for this situation is that Finland was not a member of the Council of Europe at the time, nor were references to the Council's conventions otherwise common given the country's foreign policy considerations in that period. 4 The exceptionally extensive **authority** of the **Data Protection** Board to admit exceptional permits to deviate from the provisions of the Act can be partly explained if one looks at the situation in

Footnote:
which the Personal Data File Act was first applied in practice. It was very difficult to anticipate the transition from full freedom to compile data files and record data to the present strict regulation which reflects international developments. Under the circumstances, a system of exceptional permits was a natural alternative to constant minor amendments of the legislation when data file practice had to be reconciled with the stipulations of the new Act. In the era of the European **Data Protection** Directive, it is however no longer possible to continue such a system. See Wikstrom, Oikeuskaytannon tulkinnasta (mit deutscher Zusammenfassung), p. 204. Wikstrom divides legal practice into three categories according to the strength of the claims made about it; these are open, routine, and strong situations of interpretation. In his view, an open situation arises in the case of new legislation, when both the phenomenon being regulated and the law itself are new.

Footnote:

7 A situation is relatively open when an institution exists but the norms governing it change. The changes made in the Personal Data File Act have not changed the institution as such. Directive 95/46/EC.

The reform of the Personal Data File Act in Finland is being prepared by the ten-member Personal Data Commission under the leadership of the Head of Legislation of the Ministry of Justice, Mr Pekka Nurmi. The commission has seven permanent experts and three secretaries. I myself am a member of the commission.

10 On this issue, see Ejan MacKaay's incisive presentation in Altes, Dommering, Hugenholz and

Kabel (eds), Information Law towards the 21st Century, p. 43. 11 The coming into force of the Act was staggered such that the provisions applying to **data protection** officials came into effect on 1 October 1987, and the rest of the legislation at the beginning of 1988. It was stipulated that the personal data files in use prior to the coming into force of the Act were to be converted to conform to the provisions of the Act, with a number of transitional periods being prescribed for this purpose.

Footnote:

12 In 1994, the Personal Data File Act was changed owing to opposition by the media such that only the protection of editorial files was subject to the supervision of the **Data Protection** Ombudsman. 13 In 1994, the Personal Data File Act was changed such that a permit was no longer required to compile a Who's Who publication. The justification for the permit requirement was that the connection between the publisher and the subjects of the personal data file could not be established in all cases. The Personal Data File Act requires that the controller and subject of a personal data file must have a substantive association. If an organization is putting out the publication, the requirement of association is not fulfilled if data on persons outside of the organization have been included in the work. For example, the lawyers' Who's Who, published by a company owned by the Finnish Lawyer's Association, did not fulfil the requirement of association and thus required a permit from the **data protection authorities** . The model for this provision can be found in the Swedish Data Act.

Footnote:

Konstari, Henkilorekisterilaki (Personal Data File Act), p. 11. 16 1 use the term 'linking provision' to denote a provision which directs a person applying one law

to apply a second law as well.

When the Personal Data File Act was enacted, the Access to Public Documents Act adopted the concept of the technical store. A computer store is now expressly defined as a document and a prohibition was added to the Act requiring that any party requesting data should provide an account of the purposes for which it would be used. These provisions are connected with the Personal Data File Act but do not resolve the relation between the two pieces of legislation. Government Bill, p. 56. Often, one has been content to state in a somewhat rigid fashion that right of access supersedes **data protection** . I myself have such a claim on record in the Finnish legal literature. Moreover, the joint **data protection** guide of the **Data Protection** Ombudsman's office and the Central Federation of Municipalities expresses the relation between the statutes unequivocally, stating that the Access to Public Documents Act supersedes the Personal Data File Act. Especially after both issues- **data protection** and the principle of publicity-were taken into account in the Constitution, a comment this general in nature is at best vague. The matter must

Footnote:

be examined provision by provision with due consideration given to the horizontal effect of the Personal Data File Act on other laws.

19 **Data protection** in Finland is institutionally regulated, in accordance with international practice. **Data protection** legislation provides for the special officials who deal with **data protection** matters. The structure of the system is straightforward enough. The Data Ombudsman is responsible for practical guidance and supervision, while the **Data Protection** Board is a body to which decisions of the Ombudsman may be appealed and which has extensive **authority** to issue exceptional permits. Beyond these two, there are no special officials. Decisions of the **Data Protection** Board may be appealed to the Supreme Administrative Court. 20 The decisions of the Parliamentary Ombudsman are published both in his own annual report and, in the form of summaries, in the legal databank Finlex. The above text is a translation of the bulletin published in the latter.

Footnote:

21 It is somewhat surprising that the appellate instance for decisions of the **Data Protection** Board is the Supreme Administrative Court, for today we are increasingly ready to admit that **data protection** is primarily an individual civil right, one which is part of our right to self-determination. When the Finnish legislation on **data protection** was drafted, the situation was different: the perspective adopted in the work was that of administrative officials, and the work was carried out by specialists in public law. Accordingly, the highest appellate instance is, from the standpoint of privacy, at the end of the wrong road, i.e. in a court which as a rule protects publicity. 22 In Finnish practice there has been disagreement over the extent to which a person browsing an administrative record may make notes. The outcome is-or can be the same as in the case of mass delivery. In a preliminary ruling handed down in April 1996, the Supreme Administrative Court took the view that taking notes by hand on a large body of data constitutes mass delivery. 23 The same committee also investigated the regulation on the distribution of pornographic materials. This connection might have been one important factor impeding the later consideration of privacy. It was easy to construe protection of privacy as an exceptional matter, one requiring censorship.

Footnote:

24 No detailed provisions exist in Finland on the use of the personal identity number in personal data files. The controller of the file must always determine independently whether it is necessary to include this number in the file. The special provisions which do exist on the personal identity number apply only to specific situations. The recipient's personal identity number may not be visibly indicated on a parcel or letter sent through the mail, and in mass transfer of data it may only be used in certain special situations.

25 The Press Council, an internal monitoring body of the media, is a very odd body to be issuing guidelines in this context.

26 Section 3a.1 of the Trade Register Act implemented at the end of 1993 reads as follows: 'The personal data to be recorded in the Trade Register on a natural person are complete name, personal identity number, address and citizenship. Where the person does not have a Finnish personal identity number, his/her date of birth will be entered in the register instead.' Although the Trade Register Act has no special provisions on the delivery of personal data through mass delivery, it has been interpreted as permitting delivery of data which would not be not allowed by the Personal Data File Act.

27 Points 35 and 36 of the recitals also give rather strong support for the special status of a public

person in the regulation of **data protection** .

28 Von Wright, Tarpeesta, in von Wright, Filosofisia tutkielmia (in Finnish).
Footnote:

'Who owns the information?' is a slogan of sorts which has found its way into the legal literature in a number of ways within a rather short time. It has been most visible as the title of a book by Anne Wells Branscomb.

National censuses were begun in Finland-Sweden in 1748. The present system of census information is a direct continuation of this work.

31 To date these rights have been invoked rather rarely: as of the end of 1995, the census data system had some 35,000 prohibitions on record as

against a total population of 5 millionreason

Footnote:

why so few prohibitions have been used is that people have not been properly informed of their right to forbid the use of data.

32 Compare Robertson and Nicol, Media Law, p. 172: 'The plaintiff in action to stop a publication

on grounds of confidence is claiming a right to protect privacy, or at least private property.' 33 C. Gusy has put the matter particularly well: 'Privatheit ist so eine Freiheit, nimlich die Entscheidungsfreiheit uber Regeln, Sinn und Partner von Kommunikation, und die Handlungfreiheit nach dieser Entscheidung. Sie ist insoweit eine spezifische Eigenschaft von Interaktion. Diesen Character teilt sie mit der Offentlickeit. Demnach sind beide kein Gegensatz, sondern gehen graduell ineinander ber.' Gusy, Der Schutz der Privatsphdre in der Europaischen Menschenrechtskonvention Art 8, DVR 1984 s 292.

34 Makkonen, Zur Problematik der Juridischen Entscheidung, p. 61. 35 The Personal Data File Act requires that data files must be defined before they are first used. In practice, this obligation is often neglected.

Author Affiliation:

Correspondence: Ahti Saarenpaa, University of Lapland, Faculty of Law, PB122, FIN-96101, Rovaniemi.

GEOGRAPHIC NAMES: Finland

DESCRIPTORS: Computer security; Computer privacy; Right of privacy; Information technology; Data integrity
CLASSIFICATION CODES: 4300 (CN=Law); 5200 (CN=Communications & information management); 5140 (CN=Security); 9175 (CN=Western Europe)
?

? t s9/full/5

9/9/5 (Item 2 from file: 148)

06806645 SUPPLIER NUMBER: 14886954 (THIS IS THE FULL TEXT)
The EC proposed data protection **act.**
Mei, Peter
Law and Policy in International Business, 25, n1, 305-334
Fall, 1993
ISSN: 0023-9208 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 13056 LINE COUNT: 01067

ABSTRACT: The European Community's proposed directive on personal **data protection** is aimed at reducing the international conflict of laws that may act as a barrier to economic relations. The laws of individual nations vary greatly, and the lack of harmony can restrict the activities of multinational organizations. While the proposed amendment does set consistent minimum standards of protection for all nations, the protection of individual rights may restrict the free flow of commerce.

TEXT:

I. Introduction

Technological advances have allowed modern society to store, process, and manipulate greater volumes of information than ever before. However, this new ability has also created troublesome social side effects. One such problem is the privacy intrusion on the individual when personal data is used and transmitted by organizations without the permission or knowledge of that individual. Although many countries have passed laws protecting the rights of the individual to private information,(1) if that data is sent to another country that does not possess equivalent protective laws, individuals could nonetheless be subject to potential privacy problems. As a result, many countries have passed laws restricting the flow of personal data across national boundaries.(2)

The European Community has found that divergent standards of **data protection** and transborder **data** flow restrictions can seriously impede trade in a common unified market.(3) Several of the EC countries have extremely strong **data protection** laws, while others provide little or no protection at all.(4) This has caused the placement of barriers to the free flow of information among the European countries.(5) In 1992, realizing that harmonization of the various **data protection** laws would be necessary to create a truly unified market, the European Commission released a proposed EC directive that sought to address this problem.(6) This Note examines the proposed EC directive. Part II reviews the history of European **data protection** law. Part III discusses the provisions of the proposed directive. Part IV examines its potential effects on United States companies seeking to do business in the EC. Part V proposes a course of action that frames this issue within the international arena. The Note concludes by stressing that an international accord on **data protection** must be reached, and attempts to allay fears that the proposed directive will unduly impede business transactions for U.S. multinational corporations.

II. Background of European **Data Protection** Laws

The origins of the present European **data protection** laws lie in the efforts of two organizations: the Organization for Economic Cooperation and Development (OECD) and the Council of Europe.(7) Both established influential guidelines for **data protection** and basic rules on transborder data flow.(8)

As early as 1970, the OECD has been concerned about potential effects of privacy **protection** legislation on transborder **data** flow.(9) The OECD is an organization of industrialized states spanning several continents, dedicated to promoting the economic development of its member

countries.(10) In 1978, the OECD established an intergovernmental group to investigate legal and economic problems that could arise from restricting transborder data flow, and to establish guidelines for the basic rules of **data protection** legislation.(11)

In 1980, the OECD issued voluntary guidelines for the **protection** of personal **data** and transborder data flows.(12) It was hoped that these guidelines would influence the member countries to harmonize their national legislation.(13) The OECD Guidelines stressed the importance of the free flow of information to economic development, and encouraged the removal of unjustified obstacles to international data movement.(14) The document suggested certain principles to be used in creating these laws, including the collection limitation principles, the data quality principle, the purpose specification principle, the use limitation principle, the security safeguards principles, the openness principle, the individual participation principle, and the accountability principle.(15)

As early as 1968, the Council of Europe had also started a program to study potential courses for **data protection** legislation.(16) The Council consists of European countries whose aim is to promote European unity and cooperation, with a special emphasis on human rights.(17)

The Council adopted the first regional convention on data privacy rights in 1981.(18) The focus of the document, known as the European Convention, is the protection of the individual with regard to private data.(19) The European Convention sets out a list of safeguarding standards that must be upheld by its signatory countries, but allows each country to set higher standards.(20) Because the European Convention emphasized the protection of the individual, less emphasis was placed on achieving the free flow of information.(21) The European Convention provided that the flow of information across boundaries could be interrupted if the target country did not provide "equivalent protection" for the individual.(22)

The scope of the European Convention included personal data and its processing in both the private and public sectors.(23) The Convention's basic principles state that the processed data shall be: (1) obtained and processed fairly and legally; (2) stored for specified and legitimate purposes; (3) adequate, relevant, and not excessive in relation to the purpose in which it was stored; (4) accurate; and (5) preserved only as long as needed for the intended purpose.(24) Individuals should be protected from databases that store information about their race, religion, sexual activities, political views, or criminal convictions, unless there are "adequate" safeguards against **unauthorized** disclosure or use.(25)

As of 1993, ten European countries have ratified the convention and another eight have signed without ratifying.(26) However, this has not resulted in uniform protection, as several of these countries have not subsequently implemented national **data protection** legislation.(27) Further, there are differences even among those countries that have passed **data protection** laws based on the convention.(28) This nonuniformity is the result of several factors. First, some of the legislation passed in the different countries predated the convention.(29) Second, because the European Convention was not self-executing, each individual country implemented its national legislation in dissimilar ways.(30) Last, because important but vague terms within the convention have been left undefined,(31) countries have been left to create their own definitions in their implementing legislation.

Thus, while many countries in Europe have established strong measures of protection for their citizens' rights to privacy and data integrity, legislative implementation differs from country to country.(32) To protect the rights of their citizens from being abrogated in countries with less stringent **data protection** laws, the legislation of most countries contains provisions restricting the flow of data across national boundaries. While it was hoped that the European Convention would harmonize the **data protection** laws, this desire has not been realized.(33)

Neither the OECD Guidelines nor the European Convention has succeeded in achieving the goal of harmonizing **data protection** laws in the EC. The European Community realized that divergent standards of **data**

protection could create barriers to trade within the unified market, making restrictions on transborder data flow unnecessary. In 1990, this topic was a priority issue in the European Commission's program.(34) By September of that year, the European Community had drafted a directive addressing **data protection** and transborder **data** crossings.(35)

Industry groups and European government officials objected to many aspects of the Draft Directive,(36) and the EC Economic and Social Committee delivered a critical opinion of it in April 1991.(37) The Committee on Legal Affairs and Citizens' Rights for the European Parliament, released a report on the Draft Directive that suggested many amendments,(38) more than one hundred of which were included when the European Parliament finally approved the Draft Directive in March, 1992.(39) On October 15, 1992 the Commission of the European Community revised its original draft and released an amended proposal for a directive on **data protection** .(40)

III. The Amended Proposal

The Amended Proposal draws a great deal from the European Convention.(41) Thus, it is not surprising that many of the provisions are similar. However, this document has expanded into a far-reaching proposal, **protecting** personal **data** beyond the original directive's scope, which was limited to automated data processing.

The Amended Proposal is a set of guidelines that each member state of the European Community must use to enact domestic legislation.(42) Ratification is not voluntary; the Amended Proposal provides that each EC member state "shall" enact national legislation ratifying the proposal by July 1, 1994.(43) The Amended Proposal sets only the minimum levels of mandatory protection implementation, permitting the member states to set higher standards.(44)

At this point, it may be helpful to provide definitions of some of the terms used in the Amended Proposal. "Data subject" describes the person whose personal data is to be stored or processed by another entity.(45) "Processing" refers to any operation or set of operations which are performed on personal data.(46) "Controller" refers to any natural or legal person, public **authority** or agency that processes personal data or who decides the purpose, methods, or selection of the personal data to be processed.(47) "Third party" means any natural or legal person other than the data subject or controller or the controller's **authorized** representative.(48)

A. Scope of Protection

The scope of the Amended Proposal covers personal data that is collected on individuals and held in either the private or public sectors. The Amendment Proposal removes the distinction between private and public sectors that existed in the original draft directive(49) and mandates the same treatment for both.(50)

The Amended Proposal specifies that only natural persons are protected by the provisions of the **data protection** directive.(51) Although some members of the business community feared that the **data protection** directive would also apply privacy protections to legal entities, these fears were unfounded; the Amended Proposal states that only files associated with natural persons are **protected** .(52)

Personal **data** that is regulated includes any information about a person that can be used, either directly or indirectly to identify that individual.(53) This includes information such as name, address, driver license number, age, occupation, and telephone number. Interestingly, it also includes data relating to appearance, voice, fingerprints, and genetic characteristics.(54) However, certain kinds of data are exempt from regulation if they have been compiled into statistics from which individuals can no longer be identified.(55)

The Amended Proposal protects individual privacy by regulating the use of "personal data files," which include any set of data organized to allow structured access and searches for information on individuals.(56) However, the scope of protection varies depending on whether or not the data is processed by automatic means.(57) For the automated processing of **data** , the extent of **protection** does not depend on the actual presence of

a "file."(58) The file requirement only applies when the information is to be processed manually. Any set of structured records, including paper records, fits within this provision of the directive.(59) In effect, the index card record system of a small business would be subject to the same regulation as the large computerized databases of a major corporation.(60)

Unstructured, non-electronic data would not be considered a "data file" and would not be regulated by the Amended Proposal.(61) Thus, individual letters and documents kept by a business would not be covered. However, any automated processing of data, whether part of a structured file or not, would be subject to the **data protection** directive.(62) This would include word processing documents **stored** on a personal computer.

There are two exceptions to the above definition of information that is covered by the Amended Proposal. The first exception pertains to activities outside European Community law.(63) One such example is data collected purely for national intelligence organizations.(64) The second exception applies when data is used for purely private purposes,(65) which would include purposes such as recording private notes in an electronic diary or personal address book.(66)

B. Controlling Law

The Amended Proposal also specifies which national law applies to the processing of data.(67) If the controller of the file is based in the European Community, then the applicable law is that of the country where the controller is located.(68) If the controller is located outside the EC, then the law of the country in which that controller will be using or collecting the data applies.(69) The directive further states that extra-EC controllers must designate a representative within the member state to be responsible for their obligations.(70)

C. Collecting the Information

The Amended Proposal states that the information collected on individuals must be processed in a fair and lawful manner,(71) which has been interpreted to mean, in most situations, that the information can be processed only with the permission of the data subject.(72) This principle would prevent controllers from developing and using clandestine processing operations for personal data.(73)

The information may be collected only for a specified, explicit, and legitimate purpose,(74) and must be used in a manner compatible with that purpose.(75) The purpose must be disclosed before the data is collected, and the intended use must be defined as accurately as possible.(76) A general description of intended use, such as "for general commercial use," would not be specific enough to meet the requirements of the Amended Proposal.(77) A later change in the processing use of that data is allowed only if the later use is compatible with the purpose for which the data was first collected.(78)

The Amended Proposal also limits the quantity of data collected and the duration of its storage. The data collected must be adequate, relevant, and not excessive in relation to the intended purpose for its collection - the controller should not collect data beyond what is needed for processing purposes.(79) In addition, the data should not be stored longer than necessary to achieve the processing purposes,(80) unless it is being stored for historical, statistical, or scientific reasons.(81)

Article 7 of the Amended Proposal lays out situations in which personal data may be processed.(82) Generally, personal data may be processed when the data subject has consented to the processing.(83) Consent is defined as any express indication of the data subject's agreement to the use or processing of his personal data.(84) Consent must be given freely and specifically, and may be withdrawn by the data subject at any time, but without retrospective effect.(85)

Consent is not required if the data subject has vital interests in having his data processed, but is unable to give consent.(86) This is a narrow exception for situations such as medical emergencies.(87)

Processing the data would also be allowed when necessary to the performance of a contract with the data subject, or if preliminary steps are requested by the data subject prior to entering a contract.(88) This provision is intended to allow the routine use of data by businesses for

dealing with ordinary customers without requiring consent for every transactions.(89)

Certain types of data are considered especially sensitive and are treated with higher levels of care. These special categories include personal information regarding the data subject's ethnic or racial origin, health, sexual preference, political, philosophical or religious views, or trade union membership.(90) Data of these types may be used if the data subject has consented to the processing of that data.(91) In addition, the data may also be used if the processing is performed by a foundation or a non-profit organization devoted to political, philosophical, religious, or trade union issues in the course of its legitimate activities, provided that the data subject is a member of that organization or has regular contact with that organization in connection with the organization's purposes.(92) This particular article has been subject to many different interpretations by the European states, and would be significantly harmonized by the proposed directive.(93)

D. Rights of the Data Subject

Data subjects have a basic right of access to compiled information relating to themselves.(94) Article 13 allows the data subject to obtain, at "reasonable intervals," without excessive delay or expense,[95] confirmation of the existence of such personal data regarding themselves and to receive communication of such data in an "intelligible form."(96) The data subject also has the right to be informed of the source of such data and general information about its use.(97)

The Amended Proposal grants data subjects the right to rectify any inaccurate or incomplete data regarding themselves.(98) In addition, the data subject is able to obtain the erasure or suppression of such data if it has been processed in violation of this directive.(99) However, although the controller will be prohibited from further processing or use, the controller will nonetheless be allowed to store the offending information.(100) When third parties have already been transferred inaccurate or incomplete information, the Amended Proposal provides that the data subject can see to the rectification, erasure, or suppression of the transferred data as well.(101)

Article 15 of the Amended Proposal gives data subjects the right to object on legitimate grounds to the processing of their personal data.(102) The existence of legitimate grounds depends on whether there was any legal justification for the particular processing use in question;[103] a use has legal justification if any of the requirements set out in Article 7 are met.(104) The controller must stop processing the data if there is a justified objection.(105)

The controller must give the data subject the opportunity to have personal data erased before it is disclosed to a third party or used for marketing by mail.(106) Although the opportunity must be expressly offered to the data subject,(107) the controller could satisfy this requirement through regular correspondence with the data subject without creating any special communications.(108) This obligation will apply to any situation involving mail solicitation, whether it is for commercial purposes or some form of charitable or political activity.(109)

To ensure that data subjects can effectively defend their rights and monitor the use of the data relating to themselves, Article 11 requires certain types of information to be provided to the data subject when the data is collected.(110) Information that must be disclosed includes: the purpose of processing the data;(111) whether the responses of the data subjects are obligatory or voluntary;(112) the consequences for the data subjects if they fail to reply to data requests;(113) the recipients or the category of recipients of the requested data;(114) the right of the data subjects to access the data relating to themselves and to rectify any errors;(115) and the name and address of the controller or any designated representative.(116)

Article 10 grants data subjects the right to be informed of certain kinds of information upon request.(117) This article data subjects the right to know of the existence of any processing operation and its purposes.(118) In addition, the controller must disclose the types of data used and identify any third parties to whom the data is disclosed.(119)

Also upon request, data subjects are to be notified of the controller's name and address, or those of the controller's representative.[120] Articles 10 and 11 both relate to information the controller must provide to data subjects. Whereas information covered by Article 11 must be provided on the controller's own initiative, the information covered by Article 10 need only be provided upon data subjects' request.(121)

Article 12 of the Amended Proposal lists the information a controller must provide to data subjects before data relating to themselves is disclosed to third parties.(122) This information includes the name and address of the controller or the controller's representative,(123) the purpose of the processing,(124) the categories of data disclosed,(125) the recipients of the data,(126) and the existence of the data subject's rights of access, rectification, and objection.(127) The following situations, among others, are exempt from this requirement:(128) the original ground for processing was in accordance with the Article 7(a) consent of the data subject;(129) the data subject has already been informed that the data was or might be disclosed to a third party;(130) the disclosure was made to safeguard the data subject's vital interests;(131) or the activity involved has been designated by the national legislature as exempt from this provision and adequate safeguards are present.(132)

Article 14 of the Amended Proposal lists certain circumstances in which the rights of data subjects may be restricted.(133) Restrictions may be emplaced in the interests of national security,(134) defense,(135) criminal proceedings(136) public safety,(137) a duly established paramount economic or financial interest of a member state or the EC,(138) monitoring or inspection by a public **authority** ,(139) and equivalent rights or freedoms of another person.[140] If the data subject's rights are restricted through the invocation of Article 14, the subject retains the right to require the national supervisory **authority** to ensure the lawfulness of the restriction.(141)

E. Automated Decisions

Article 16 of the Amended Proposal declares that individuals generally have the right to not be subjected to adverse decisions based solely on the automated processing of a defined personality profile.(142) The intent of the provision is to prevent the use of sophisticated software system from making mechanical decisions about an individual without the actual input of human judgment.(143) Three conditions must be satisfied before a data subject can invoke this right.(144) First, there must be a decision involving potentially adverse consequences pending against the data subject.(145) Second, the decision must result solely from automated processing.(146) Third, the processing must use variables which determine a standard profile based on information collected on a data subject.(147)

The data subject must accept a negative automated decision: (1) if the decision is made under a contract between the controller and the data subject or in the conclusion of that contract, provided that any requests of the data subject are satisfied;(148) or (2) if there have been suitable safeguards enacted to protect his legitimate interests.(149) However, when an adverse decision is reached based on any automated processing decision, Article 13(5) grants the data subject the right to be informed of the reason.(150)

F. Obligations of the Data Controller

The controller must take appropriate technical and organizational measures to ensure the security of the data under his control, in order to prevent the **unauthorized** access, alteration, disclosure, or any other types of **unauthorized** processing to be performed on personal data.(151) In addition, the controller should act to prevent accidental or unlawful loss or destruction of that data.(152)

The controller of a processing operation must notify the national supervisory **authority** before carrying out any wholly or partly automatic processing operation.(153) The individual countries will be free to determine whether they will apply these same measures to manually maintained files.(154) The national legislatures are to determine the amount of information to be supplied by the controller, but at a minimum the following are required: the names and addresses of the controller and any representative;(155) the purpose of the processing;(156) the categories

of data subjects;(157) a description of the categories of data to be processed; (158) the names or categories of third parties to whom the data might be disclosed;(159) any proposed transfers to third countries;(160) and a description of measures taken by the controller to ensure adequate **protection** of **data** in the controller's possession.(161)

The Amended Proposal attempts to simplify notification procedures. Some organizations have multiple processing operations that serve or relate to a common purpose or a set of common purposes. The proposal permits a single notification to cover the set of operations, rather than requiring separate notification for each step.(162) This would apply to situations such as the processing operations associated with the management of loans - a single notification would be required for the multiple steps, which might include the registration of the application, the background investigation, the approval process, and the tracking of the legal proceeding.(163)

The Amended Proposal also allows the member states to create certain categories of operations that will be exempt from or subject to lesser reporting requirements.(164) These categories include only processing operations that will not adversely affect the rights and freedoms of data subjects.(165) Many of the operations that organizations engage in are simple, standard operations or are strictly defined in legal terms. Some of the examples listed in the Amended Proposal are "the production of correspondence or papers by word processing, the satisfaction of legal, accounting, tax, or social security duties, or the consultation of document services accessible to the public."(166)

G. Transfer to Third Countries

A basic principle of the Amended Proposal is that a data transfer to a third country may take place only if that third country provides an "adequate level" of protection.(167) The adequacy of the protection provided by that third country is to be evaluated in light of all circumstances surrounding a data transfer operation.(168) The primary factors to be considered are the purpose and duration of the processing operation, the domestic legislation in effect, and the professional rules that are complied with in the third country.(169)

There are several exceptions to the general requirement of adequacy.(170) A transfer is allowed to a third country that does not provide adequate protections if the data subject has consented in order to take steps preliminary to entering a contract.(171) The transfer also would be allowed if necessary for the performance of a contract between the controller and the data subject, provided that the data subject was informed that transfer to a third country without adequate protections might be necessary to perform the contract.(172) As a further exception to adequacy, transfers that protect the vital interests of the data subject are permitted whether or not the recipient country can ensure adequate levels of protection.(173)

The supervisory **authority** of each member state must determine whether a third country provides an adequate level of protection and whether a ban on data transfers should be implemented.(174) If the member state determines that a third country does not provide adequate protection, it must inform the European Commission.(175) The Commission might decide that a third country does ensure an adequate level of protection by virtue of its international commitments or its domestic laws.(176) However, if the Commission finds that the protection provided in the third country is inadequate and could harm the interests of the EC or a member state, it may enter into negotiations with that third country to attempt to remedy the situation.(177)

Even if the Commission finds that a third country does not provide an adequate level of protection, a member state can still **authorize** a transfer to that country if the controller wanting to transfer the data provides sufficient evidence, most likely in the form of contractual guarantees, that the data subjects concerned will be able to effectively exercise their rights granted by the Amended Proposal.(178) In this situation, the member state must inform the Commission and the other member states prior to approving the transfer.(179) If an objection is made by the Commission or any member state, the Commission is to take "appropriate measures,"(180) which may be to prohibit the transfer, create additional

conditions that must be met, or enter negotiations with the controller to ensure a satisfactory solution for the whole Community.(181)

IV. DO U.S. COMPANIES HAVE A POTENTIAL PROBLEM?

The implementation of the Amended Proposal could have serious consequences for U.S. companies seeking to do business in the EC.(182) Most U.S. multinational corporations are not accustomed to restrictive **data protection** laws like those proposed for the EC and, moreover, lack the internal organization needed to comply with such laws.(183) U.S. companies complain about the European data inspection ministers who monitor and restrict transfers of information abroad,(184) and argue that although some restrictions can be justified on privacy grounds, the heightened provisions of the Amended Proposal could unduly impede international business transactions.(185)

Most major U.S. multinational corporations are product-oriented operations that need central control over manufacturing operations and marketing information.(186) Sophisticated international data communication networks are necessary to handle the tremendous volume of data that is processed and stored by these corporations.(187) The types of data transferred through these networks range from purely business information, such as purchase orders and product information, to more personal information, such as employee health and benefits records.(188)

An example may illustrate some of the potential problems. A typical manufacturer with either sales or manufacturing organizations in Europe is likely to have an information network connected to its European division. The data transferred would contain information about accounts receivable, customer orders, customer addresses, sales data, employee information, production schedules, and the like. Suppose the marketing database used by the European division is down because of hardware problems, and the backup processing center for this company is located in the United States. If the **data protection** laws of the United States do not meet the EC standard of adequate protection, the marketing database could not be sent to the backup computer center to process customer orders unless each person in that database is first contacted. This could cause considerable losses to the company if it fails to meet product and shipping deadlines.

This situation has already arisen for a U.S. manufacturer in Europe. IBM was recently prevented from transferring employee records from France to Italy because of France's concern that Italy had inadequate personal **data protection** .[189] This type of interruption in information flow creates management problems, raises costs, and impedes customer service.(190)

The Amended Proposal will create difficulties for product-oriented corporations, but its greatest impact may be on U.S. service industries.(191) In the last few decades, the service sector has become a significant part of the U.S. economy,(192) and the EC is its largest export market.(193) The service industry owes much of its growth to the advances made by computers and telecommunications in the world business economy,(194) which now permit many complex international transactions to be performed in a fraction of the time previously needed.(195) Some of the service areas that may be affected by the Amended Proposal are telecommunications, banking, export finance, investment counseling, insurance, management consulting, legal advice, credit industries, and the information services companies.(196) Due to the unique nature of service industries, disruptions in the international flow of information could have a particularly harmful impact on these businesses.(197)

The international banking, finance, and credit industries comprise a significant part of the service sector in the United States.(198) These institutions rely heavily on international data flow to conduct their business.(199) The typical international credit institution will process millions of transactions over global data networks,(200) involving precisely the types of personal data that the Amended Proposal means to cover.(201) It usually has a primary data center that handles a variety of transactions through requests originating from smaller data centers located around the world.(202) The communications network for this type of institutions is critical to its operation.(203) If this information flow is disrupted, the institution could not provide services to its

customers.(204) Consider the case of a credit card issuer whose computer operations are located in several countries and whose customers travel to the EC. It would become an administrative headache for that company to have to determine for each individual transaction whether it could transmit credit information for a particular customer to a particular country, and whether it would need prior customer consent to do so.

A. Transborder Data Crossings into the United States

Does the United States have adequate levels of protection? The Amended Proposal states that transfers to third countries can take place only if the third countries ensure an adequate level of protection.(205) To assess whether the United States meets the European standard, the backgrounds of the approaches taken by the United States and the EC must be compared.

Most European countries have taken an omnibus approach in creating their **data protection** legislation, granting a general protection against automatic processing of personal data.(206) The Amended Proposal takes this approach as well.(207) This method usually establishes a broad framework for the protection of the individual, with **data protection** laws regulating a wide range of uses and situations.(208) The laws do not target organizations or operations that seem likely to cause harm to an individual if data relating to him is improperly processed. They apply without regard to the type of organization holding the data, the type of operation involved, or the likelihood of the potential harm to the individual.(209) The omnibus approach sets forth principles that set a specific level of protection in any given situation.(210) The Amended Proposal also **protects data** without distinguishing whether it is located in the private or public areas.(211)

This omnibus approach typically creates a national administrative organization that regulates the use, storage, and maintenance of personal data and has broad powers to supervise the compliance of **data** -collecting groups with the **data protection** laws.(212) The provisions of the Amended Proposal call for the creation of national supervisory bodies to regulate the use and transfer of personal data and other associated processing operations.(213)

The United States has taken a sectoral approach rather than an omnibus approach, attempting to focus its laws in specific areas where the use of personal data could have harmful effects.(214) This is a targeted, sector-by-sector approach that tries to take the narrowest measure possible to avoid excessive regulation.(215) The United States currently has legislation protecting the privacy of the individual at the federal, state, and local levels,(216) creating rights to be enforced privately through the court system, rather than publicly through oversight by a specially created agency.(217)

The United States actually pioneered the concept of privacy protection for the individual.(218) U.S. law first applied privacy rights to tort law, mainly in the areas of physical privacy and damage to reputation or name.(219) However, the rapid growth of computer technology, combined with the greater use of information services in daily life, spurred development of data privacy policies in the 1970s.(220) In 1974, the United States enacted a law designed to safeguard the privacy of personal records held by the federal government.(221)

The basic principles underlying the Privacy Act of 1974 coincide with many of the principles in the Amended Proposal.(222) They are: the openness principle, which states that there should be no personal data collection system kept in secrecy; the individual access principle, stating that an individual whose records are being kept by an organization should be allowed to see those records; the individual participation principle, stating that an individual whose records are being kept has the right to correct or amend those records; the collection limitation principle, stating that there should be limits on the type of information collected and the manner in which it is collected; the use limitation principle, stating that there should be limits on an organization's internal use of personal data; the disclosure limitation principle, stating that limits should be placed on disclosure to third parties of information collected about the individual; the information management principle, stating that an

organization should bear affirmative responsibility for establishing responsible practices for collecting and maintaining the information collected; and the accountability principle, stating that a record-keeping organization should be accountable for its data policies, practices, and systems.(223)

Congress later passed several statutes focusing on particular areas that were believed to need special protections. One example is the Financial Privacy Act of 1978, which regulates the release of consumer information to federal agencies.(224) Another is the Fair Credit Reporting Act, (225) which protects the privacy of an individual's financial records by requiring federal agencies to obtain a court order before they can access those records without the individual's consent.(226) A third example is the Family Educational Rights and Privacy Act, which prohibits government access to information on a person's education without authorization or a court order.(227)

These three laws all **protect** the individual's **data** privacy rights from being invaded by the federal government. Federal laws also address aspects of personal data privacy in the private sector. Some of the more recent laws include the Fair Credit Billing Act,(228) the Fair Debt Collections Practices Act,(229) and the Electronic Fund Transfers Act.(230 However, these acts often fail to focus on many of the principles of data privacy.(231) The credit laws do not adequately address consent and notice issues for the collection of personal data,(232) and the electronic funds laws focus primarily on data accuracy without giving proper consideration to other privacy issues such as consent and disclosure.(233) While many of the principles behind the federal privacy laws under the United State's sectoral approach seem to coincide with the provisions of the European standards, actual implementation of these principles seems to miss vital areas of protection.(234)

Certain industry groups have made significant efforts to self-regulate their activities, perhaps in part to dissuade Congress from enacting mandatory government regulation.(235) The Direct Marketing Association, a trade association with membership of more than 3000 corporations, first established a program in 1971 that compiled a list of consumers who wished to have their names removed from direct marketing mailing lists.(236) As of 1990, approximately 600,000 people were on this list.(237) DMA estimates that placement of a name on this "opt-out" list will remove the consumer from ninety percent of all national direct marketing lists.(238)

Even with the **data protection** measures presently in place, many feel that these laws and self-imposed regulations do not adequately protect the public. Commentators find that the present laws simply will not work without a national supervisory body to coordinate protection efforts.(239) The United State's approach is criticized because no general framework exists to provide uniform **protection** for personal **data** ,(240) although individual federal statutes cover some situations.(241) There is also a smattering of state statutes seeking to provide protection in other areas, creating a confusing patchwork of federal and state guidelines and statutes that inevitably leaves significant gaps in protection for many individuals.(242) V

Areas not specifically targeted for protection by legislation can be exploited by commercial organizations, as was illustrated by the recent attempt by Lotus to market CD-ROM discs containing consumer profiles on approximately 120 million individuals and 80 million households.(243) Although Lotus developed a comprehensive **data protection** plan on its own initiative, it was forced to abandon the project when consumer groups and many customers vehemently protested the effort.(244)

The Amended Proposal gives many rights to data subjects that are not presently granted to individuals in the United States. For instance, basic rights of access and rectification that permit data subjects to access, correct, or complete information collected on them are not always granted under U.S. laws. A recent survey of major U.S. corporations found that seventy-eight percent of the respondents check, verify, or supplement information about their employees.(245) However, only forty-four percent of these companies allow the employees to see this information, and only

thirty percent have policies that allow information to be corrected if incomplete or erroneous.(246)

Unrestricted transfers of personal data profiles occur every day in the United States because of incomplete legal protections for records about consumer transactions.(247) Companies are generally able to compile, use, sell, or trade this information without restriction or notice to the consumer.(248) The daily load of junk mail that most households receive attests to this fact.

The unregulated handling of sensitive data by private organizations in the United States is sure to be another concern of the EC.(249) For instance, job injury reporting databases in the United State(250) are used by employers to screen job applicants for their health histories.(251) These databases often become "blacklists," making it difficult for people with certain kinds of health problems to find employment.(252)

It is apparent that there is concern about the adequacy of **data protection** within the United States as well.(235) A recent poll shows that seventy-nine percent of the U.s. public have concerns about personal privacy, and seventy-one percent feel that they have lost all control over how personal information about them is circulated and used by businesses.(254)

The United States' **data protection** laws may not meet the EC standards of adequacy.(255) Because the United States has taken the sectoral approach in enacting **data protection** legislation, it is likely that the EC will take a sector-by-sector approach in deciding whether data transfers to the United States will be allowed.(256) Data transfers would be permitted in sectors in which U.s. law provides strong protection, but in sectors with less **protection** , **data** transfers may be barred.

The United States may have difficulty complying with Article 16 of the Amended Proposal. This is the provision that forbids adverse decisions against individuals from being based solely on automated processing.(257) According to the Amended Proposal, any such adverse decision must be reviewed by a human being before it may be issued.(258)

Many categories of decision making are based strictly of factual criteria and can be processed more quickly and efficiency if performed by a computer.(256) Examples include systems that check for a minimum annual income before issuing a credit card, or a minimum income-to-debt ratio before approving a personal loan. Such decision making would be permitted by the Proposed Amendment to justify positive responses, but every negative response requires that the decision result from personal, as well as computer, analysis.(260)

B. How U.S. Companies Can Prepare for New EC Laws

Companies can take several steps in order to prepare for compliance with the Amended Proposal. The company should determine whether it has any data operations that will be covered by the Amended Proposal. Any sort of records processing in electronic form will fall under the Amended Proposal.(261) Any form of manual record keeping that is in a structure format must also comply with the **data protection** laws.(262) Companies must then determine whether their processing of that data is lawful under the provisions of the Amended Proposal. Two issues these firms must address are whether the collected information is being held longer than is allowed and whether the data that is collected is directly relevant to the intended use.(263) Companies also must take special care processing data that is considered sensitive.(264)

Companies then must organize the information they are required to provide to the national supervisory **authority** of each country.(265) It is important that they determine whether those countries have simplified procedures in place to relieve some of the notification requirements.(266) Some commentators estimate that simplified requirements could excuse eighty percent of a company's processing operations from the notification provision.(267) An accounting of which information must be given to the data subject in each country must also be organized, and procedures should be in place to handle the data subjects' rights of access and rectification.(268)

If the interaction with the data subject could result in any later

transfers of data to third countries that may not have adequate levels of protection, notice of this possibility should be given to and consent should be requested from the data subject at the time of collecting the data.(269) Consent should be obtained, even though companies might find that many of the transfers are required by contractual necessity, and thus would be exempted from many of the reporting and consent requirements.(270)

Any organizations that transfer customer lists to other companies, including many commercial and direct marketing companies, will be affected by the Amended Proposal. Every customer must be given the opportunity to "opt out" of new mailing list arrangements.(271) If data subjects opt out, their names can no longer be used for any further purposes,(272) except as permitted by Article 7 of the Amended Proposal.

Some companies may find it easier to maintain several smaller localized databases rather than creating larger centralized computer systems. This would lower the probability that differing national **data protection** laws might interrupt information flow. Many companies are already moving in this direction.(273)

Computer network, system, and database managers will need to evaluate the security of their systems. The Amended Proposal stresses the importance of maintaining certain levels of security measures for systems that store or process personal data.(274)

Many companies will find that compliance with the proposed directive will result in greater expenses.(275) Some data flow will be restricted if processing centers are located in countries without adequate levels of protection,(276) and many procedures will have to be changed to secure the rights granted to data subjects in the Amended Proposal.(277)

V. The International Approach

On an international level there are at least two options the United States should consider if the Amended Proposal is implemented and becomes a barrier for the transactions of U.S. multinational companies.(278) One option is to negotiate an agreement directly with the EC; the other is to encourage the creation of an international accord.(279)

The United States could attempt to negotiate with the European Commission for an agreement on data transfers between the U.S. and the member states. The Amended Proposal provides for the possibility of a negotiated agreement if a country does not meet the adequacy standard.(280) This could be a bilateral agreement with the EC, or it could be a set of agreements between the United States and individual member states of the EC. It is unclear what standards of protection the United States must adopt before an agreement can be reached.(281)

Another option available to the United States is to place this subject on the agenda for international trade talks within future rounds of GATT negotiations.(282) **Data protection** legislation can act as a trade barrier by impeding transborder data flow, and it has been suggested that some nations have imposed these laws precisely to develop their internal industries by increasing the costs to foreign companies or preventing them from performing certain operations.(283)

Concerns of U.S. multinational corporations that the Amended Proposal may be motivated by protectionist intent are not completely unfounded. For instance, an incident occurred several years ago involving U.S. companies leasing communication lines from the German post and telegraph administration, the Bundespost.(284) At the time, there was extreme concern in the European countries that the dominance of U.S. companies in certain information and computer industries could have serious consequences for other nations' economic, social, and cultural lives. 285 The Bundespost indicated that firms leasing communication lines must utilize computer facilities within the country.(286) This was intended to encourage the growth of domestic data processing centers while discouraging the expansion of foreign companies.(287)

Recent rounds of the GATT negotiations have not fully addressed data privacy issues.(288) Although the Uruguay Round included some discussion regarding the financial services industry,(289) this industry is only one of many affected by **data protection** legislation. An international accord must be reached specifically addressing the **data protection** issue and the question of how to maintain unrestricted flows of data across

national boundaries.

The Amended Proposal for an EC directive on **data protection** represents an attempt to harmonize the various **data protection** laws within the European Community. Not all EC countries have **data protection** laws, and those jurisdictions that do have them provide for differing levels of protection and restrictions. These inconsistencies have led member states to restrict transborder data flow, which may interfere with the goal of a common unified market.

Although the amended Proposal attempts to remedy existing problems, it is likely to create new ones as well: it grants strong rights to individuals, which could become barriers to companies seeking to do business in the EC, and many provisions in the Amended Proposal are subject to different interpretations by the EC member states, which could create more of the incompatabilities that the directive is meant to prevent.

Nevertheless, in spite of these problems and the inevitably increased costs of compliance, it is possible for U.S. multinational companies to work within the Amended Proposal. The proposed EC directive has controversial provisions, but it is a good springboard for the international community to attempt to reach an agreement on the **data protection** issue. The urgency to do so will only increase as the pace of technology continues to create a greater dependence on the free flow of international data>

VII. Update

The Amended Proposal was to be presented to the EC Council of Ministers at the Council's International Market and Consumer Affairs meeting in November 1993.(290 While several significant issues and concerns must still be discussed, the Amended Proposal has been given a highly favorable reception by EC experts and a broad consensus has emerged that these **data protection** rules are needed at the Community level.(291) The European Community hopes that a common position regarding the Amended Proposal can be agreed upon during the Council's meeting in December 1993,(292)

(1.) See, e.g., Patrick E. Cole, New Challenges to the U.S. Multinational Corporation in the European Economic Community: **Data Protection** Laws, 17 N.Y.U.J. Int'l L. & Pol. 893, 902-08 (1985) (discussin **data protection** laws in Sweden, France, the United Kingdom, Belgium, and (Germany). (2.) See, e.g., Joel R. Reidenberg, The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services, 60 Fordham L. Rev. 137, 140 n.16 (1992). (3.) A.C. Evans, European **Data Protection** Law, 29 Am.J.Comp.L. 571, 574-75 (1981). (4.) France and Germany have possibly the strictest laws in this area, while Greece, Belgium, and Italy have almost none. See Cole, supra note 1, at 901-08 (1985) (describing the various **data protection** laws in the European countries); Patrick Oster, Privacy vs. Marketing: Europe Draws the Line, Bus. Wk., June 3, 1991, at 128, 128. (5.) An example of this occurred in 1989 when Fiat managers in France attempted to transfer personnel records from France to their home offices in Italy. The French **authorities** initially halted this transfer because Italy has no personal **data protection** laws, while France has high levels of protection. Oster, supra note 4. The solution was a contractual arrangement by Fiat to assure certain protections for the information. Id. (6.) Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Preamble, 1992 O.J. (C 311) 30 [hereinafter Amended Proposal]. (7.) Cole, supra note 1, at 900. (8.) Id. at 896. (9.) Michael D. Kirby, Transborder Data Flows and the "Basic Rules" of Data Privacy, 16 Stan.J. Int'l L.27, 42 (1981). (10.) Reidenberg, supra note 2, at 144. The members of OECD represent a diverse group of nations including Japan, the United States, New Zealand, Canada, Australia, and most of the countries of Western Europe. Frits W. Hondius, Data Law in Europe, 16 Stan. J. Int'l L. 87, 91 (1981). (11.) Kirby, supra note 9, at 43. (12.) Organization for Economic Cooperation and Development, Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, O.E.C.D. Doc. (C 58 final) (Oct. 1, 1980) [hereinafter OECD Guidelines]. (13.) Id.

Preamble. (14.) See Reidenberg, supra note 2, at 142; OECD Guidelines, supra note 12, pt. 3. (15.) OECD Guidelines, supra note 12, pt.2. (16.) Hondius, supra note 10, at 91. (17.) See Reidenberg, supra note 2, at 144. (18.) Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Europ. T.S. No. 108 [hereinafter European Convention]. (19.) Id. art. 1. (20.) See id. chs. 1, 2; Reidenberg, supra note 2, at 144-46. (21.) See Reidenberg, supra note 2, at 144. Compare with the OECD Guidelines, which focused on encouraging international data flow. See supra note 12 and accompanying text. (22.) European Convention, supra note 18, art. 12. See Reidenberg, supra note 2, at 161-62. However, the term "equivalent" is not defined within the document. Id. at 162. (23.) European Convention, supra note 18, art. 3(1). (24.) Id. art. 5. (25.) Id. art. 6. (26.) Reidenberg, supra note 2, at 144 n. 38. The 10 ratifying countries are Austria, Denmark, France, Germany, Ireland, Luxembourg, Norway, Spain, Sweden, and the United Kingdom. The eight who signed without ratifying are Belgium, Cyprus, Greece, Iceland, Italy, the Netherlands Portugal, and Turkey. Id. (27.) See supra note 4. (28.) Reidenberg, supra note 2, at 148. (29.) Id. (30.) Id. (31.) Examples include terms such as "equivalent protection" and "adequate" levels of protection. Id. at 161-62. See also Evans, supra note 3, at 580-81. (32.) See Hondius, supra note 10, at 97-100; Kirby, supra note 9, at 39. (33.) Evans, supra note 3, at 580-81. (34.) See Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, 1990 O.J. (C 277) 3 [hereinafter Draft Directive]; Olga Estadella-Yuste, The Draft Directive of the European Community Regarding the **Protection** of Personal **Data** , 41 Int'l & Comp. L.Q. 170, 170-72 (1992). (35.) See Estadella-Yuste, supra note 34, at 172. (36.) See Jan. M.A. Berkvens, **Data Protection** Initiative, 11 Int'l Fin. L. Rev. 12 (1992). (37.) Opinion on the Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, the Proposal for a Council Directive Concerning the **Protection** of Personal **Data** and Privacy in the Context of Public Digital Telecommunications Networks, in Particular the Integrated Services Digital Network (ISDN) and Public Digital Mobile Networks, and the Proposal for a Council Decision in the Field of Information Security, 1991 O. J. (159) 38. (38.) Session Documents Eur. Parl., PE 148.286/fin (Jan. 15, 1992), Doc. No. A3-0010/92 (hereinafter Session Documents]. (39.) Amendments, Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, 1992 O.J. (C 94) 173 [hereinafter Amendments to Draft Directive]; see also Berkvens, supra note 36, at 12. (40.) Amended Proposal, supra note 6. (41.) Before preparation of its own directive, the European Commission had encouraged its members to adopt the Council of Europe's convention, discussed above in the text accompanying notes 15-30. Estadella-Yuste, supra note 34, at 172. (42.) See Amended Proposal, supra note 6, art. 35(1). (43.) Amended Proposal, supra note 6, art. 35(1). (44.) It seems in some ways, the European Commission may be setting itself up for additional incompatibility problems, as many areas of the Amended Proposal require member states to establish their own levels of protection, which could diverge significantly. (45.) Amended Proposal, supra note 6, art. 2(a). (46.) Id. art. 2(b). (47.) Id. art. 2(d). (48.) Id. art. 2(f). (49.) In the original draft directive, "public sector" referred to organizations, **authorities** , or entities of an EC member state governed by public law, whereas "private sector" referred to natural or legal persons or associations engaged in industrial or commercial activities. Draft Directive, supra note 34, arts. 2(g), 2(h). The original directive had separate sections that created slight differences in the treatment of private and public sector files. See id. chs. 2, 3. The European Parliament felt there were too many loopholes in the original directive for public sector entities, and that these exceptions could defeat the purpose of **data protection** legislation. Session Documents, supra note 38, [paragraph] 12. This amendment by the European Parliament was later partially adopted by the Commission. See Amended Proposal, supra note 6, art. 3(1); Amendments to Draft Directive, supra note 39, amend. 21. (50.) Amended Proposal, supra note 6, art. 3(1). (51.) Id. arts. 2(a), 3(1). (52.) See Estadella-Yuste, supra note 34, at

172; Commentary on the Articles, Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, COM(92) 422 final at 9 [hereinafter Commentary on Amended Proposal]. (53.) Amended Proposal, supra note 6, art 2(a). (54.) Commentary on Amended Proposal, supra note 52, art. 2(a). (55.) Id. art. 2(c). (56.) Amended Proposal, supra note 6, art. 2(c). (57.) Id. art. 3. The Amended Proposal treats procedures involving both automatic and manual processing as automatic processing. Commentary on Amended Proposal, supra note 52, art. 3. (58.) Id. art. 3. (59.) Id. (60.) The same restrictions placed on a major corporation to protect the individual would arguably be unduly restrictive and probably unnecessary when applied to a small business. One such example would be the registration and notification requirements of the draft directive. Some smaller businesses might find the costs of complying with these requirements prohibitive. However, there is some room for the member states to create simplified procedures for smaller businesses. Se Amended Proposal, supra note 6, art. 19 (allowing member states to simplify reporting requirements for certain categories of data). (61.) Commentary on Amended Proposal, supra note 52, art. 3. (62.) Id. (63.) Amended Proposal, supra note 6, art. 3(2). (64.) Commentary on Amended Proposal, supra note 52, art. 3. (65.) Amended Proposal, supra note 6, art. (3)2. (66.) Commentary on Amended Proposal, supra note 52, art.3. (67.) Amended Proposal, supra note 6, art. 4. (68.) Id. art. 4(1)(a). (69.) Id. art. 4(1)(b). For example, if the controller of the data resides in the United States but the data terminals used by that organization are located in the United Kingdom, then the applicable laws of the United Kingdom apply. (70.) Id. art. 4(2). (71.) Amended Proposals, supra note 6, art. 6(1)(a). (72.) Berkvens, supra note 36, at 12. (73.) Commentary on Amended Proposal, supra note 52, art. 6. (74.) Legitimate purposes are those uses allowed under either the Amended Proposal or domestic legislation of the particular state. Id. art. 6(1)(b). (75.) Amended Proposal, supra note 6, art. 6(1)(b). (76.) Commentary on Amended Proposal, supra note 52, art. 6(1)(b). (77.) Id. (78.) Id. art. 6(1)(d). (79.) Amended Proposal, supra note 6, art. 6(1)(c). (80.) Id. art. 6(1)(e). (81.) Id.; Commentary on Amended Proposal, supra note 52, art.6. (82.) Amended Proposal, supra note 6, art. 7. Article 7 states that:

> Member states shall provide that personal data may be processed only if: (a) the data subject has consented; (b) processing is necessary for the performance of a contract with the data subject, or in order to take steps at the request of the data subject preliminary to entering the contract; (c) processing is necessary in order to comply with an obligation imposed by national law or by Community law; (d) processing is necessary in order to protect the vital interests of the data subject; (e) processing is necessary for the performance of a task in the public interest or carried out in the exercise of public **authority** vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary in pursuit of the general interest or of the legitimate interests of the controller or of a third party to whom the data are disclosed, except where such interests are overridden by the interests of the data subject.

(83.) Id. art. 7(a). (84.) Id. art. 2(g). Some had expressed concern whether the directive required consent to be given in writing. The Amended Proposal now makes clear that consent can be given either orally or in writing. Commentary on Amended Proposal, supra note 52, art. 2(g). (85.) Amended Proposal, supra note 6, art. 2(g). The data subject may withdraw his consent at any time, but the Amended Proposal limits retrospective effects to prevent operations that were lawful when carried out from being declared unlawfully retrospectively. Commentary on Amended Proposal, supra note 52, art. 2(g). (86.) Amended Proposal, supra note 6, art. 7(d). (87.) Commentary on Amended Proposal, supra note 52, art. 7(d). (88.) Amended Proposal, supra note 6, art. 7(b). (89.) In the original Draft Directive, consent was the major basis for legal processing of data, and routine processing of data by businesses required consent by each data subject. Draft Directive supra note 34, art. 5(b). Industry groups spent millions of dollars lobbying to have the consent requirement, along with other measures of the directive, removed or amended. Harry Chevan, Privacy Battles

Overseas, Computer Age, Mar. 1992, at 49, 49. In the amended version, consent is no longer the primary criterion, but only the first of several alternatives. Commentary on Amended Proposal, supra note 52, art. 7(b). (90.) Amended Proposal, supra note 6, art. 8(1). (91.) Id. art. 8(2)(a). (92.) Id. art. 8(2)(b). (93.) See Estadella-Yuste, supra note 34, at 173. (94.) Amended Proposal, supra note 6, art. 11(1)(e). (95.) The data controller will be allowed to charge the data subject a reasonable fee, not to exceed actual costs. Commentary on Amended Proposal, supra note 52, art. 13. (96.) Amended Proposal, supra note 6, art. 13(1). It will be left to individual domestic legislatio of the EC Countries to interpret the terms "reasonable interval" and "intelligible form." Commentary on Amended Proposal, supra note 52, art. 13. This could cause certain incompatabilities among the countries. (97.) Amended Proposal, supra note 6, art. 13(1). (98.) Id. art. 13(3). (99.) Id.; see also Commentary on Amended Proposals, supra note 52, art. 13. (100.) Storage will only be allowed for archival purposes. Commentary on Amended Proposal, supra note 52, art. 13 (101.) Amended Proposal, supra note 6, art. 13(4); Commentary on Amended Proposals, supra note 52, art. 13. (102.) Amended Proposal, supra note 6, art. 15(1). (103.) Commentary on Amended Proposals, supra note 52, art. 15. (104.) For the provisions of Article 7, see supra note 82. (105.) Amended Proposal, supra note 6, art. 15(2). (106.) Id. art. 15(3). This is the "opt-out" provision of the Proposal, in which consumers are given the opportunity to opt out of mailing lists that are sold or passed among companies. This only applies to situations involving written mail. Commentaryon Amended Proposal, supra note 52, art. 15. Protections for solicitations made through telecommunications channels are provided for in the amended proposals for a Directive for protections in the context o telecommunications networks. Id. (107.) Amended Proposals, supra note 6, art. 15(3). (108.) Commentary on Amended Proposal, supra note 52, art. 15. (109.) Id. (110.) Id. art. 11. (111.) Amended Proposal, supra note 6, art. 11(1)(a). (112.) Id. art. 11(1)(b). (113.) Id. art. 11(1)(c). (114.) Id. art. 11(1)(d). (115.) Id. art. 11(1)(e). (116.) Id. art. 11(1)(f). (117.) Id. art. 10(1). (118). Id. (119.) Id. (120.) Id. (121.) See Commentary on Amended Proposal, supra note 52, arts. 10, 11. (122.) Amended Proposal, supra note 6, art. 12(1). (123.) Id. art. 12(1)(a). (124.) Id. art. 12(1)(b). (125.) Id. art. 12(1)(c). (126.) Id. art. 12(1)(d). (127.) Id. art. 12(1)(e). (128.) Id. art. 12(2). (129.) Article 12 applies only in cases referred to in Article 7(b), (c), (e), and (f). Id. art. 12 (1). Article 7(a) covers the case in which the data subject consents. For the text of Article 7, see supra note 82. (130.) Amended Proposal, supra note 6, art. 12(2). (131.) Commentary on Amended Proposal, supra note 52, art. 12. This is a narrow exception for cases such as medical emergencies in which personal records need to be released **without permission** . Id. (132.) The drafters envisioned this exception to apply in limited cases, for example, to prevent the work of humanitarian organization from being obstructed. Id. (133.) Amended Proposal, supra note 6, art. 14. It is up to the member states to define the terms of these exceptions through legislation. Commentary on Amended Proposal, supra note 52, art. 14. (134.) Amended Proposal, supra note 6, art. 14(1)(a). This means the protection of national sovereignty from both internal and external threats. Commentary on Amended Proposal, supra note 52, art. 14. (135.) Amended Proposal, supra note 6, art. 14(1)(b). (136.) Id. art. 14(1)(c). "Criminal proceedings" refers to the prosecution of crimes already committed. Commentary on Amended Proposal, supra note 52, art. 14. (137.) Amended Proposal, supra note 6, art. 14(1)(d). (138.) Id. art. 14(1)(e). This refers to economic measures taken by the member countries, such as exchange controls, foreign trade controls, and tax collection. Commentary on Amended Proposal, supra note 52, art. 14. The Commentary also states that only a "substantial interest" of this kind would justify a restriction on individual rights, id., but "substantial" is not defined. (139.) Amended Proposal, supra note 6, 14(1)(f). (140.) Id. art. 14(1)(g). Some examples of other persons' interests are those of the controller himself, trade secrets of others, professional rules of confidentiality, court proceedings, and the protection of human rights. Commentary on Amended Proposal, supra note 52, art. 14. (141.) Amended Proposal, supra note 6, art. 14(2). This

requirement is an additional control to ensure that a series of checks and inspections are in place to prevent unlawful restriction of individual rights. Commentary on Amended Proposal, supra note 52, art. 14. (142.) Amended Proposal, supra note 6, art. 16(1). (143.) Commentary on Amended Proposal, supra note 52, art. 16. (144.) Id. (145.) Id. art. 16(1). (146.) Id. art. 16(ii). For example, this second condition is met if an employer rejects an employee solely on the basis of a computerized analysis. Id. (147.) Id. art. 16(iii). The processing must involve personality profiles determined by standard variables about the data subjects and a rating system using those profiles. Thus, the refusal to permit a withdrawal from an automated cash machine when the account is empty would not apply because that decision is based on a specific piece of data regarding that particular person - a ban balance - not on a generic personality profile. Id. (148.) Amended Proposal, supra note 6, art. 16(2)(a). (149.) Id. art. 16(2)(b). (150.) Id. art. 13(5). (151.) Id. art. 17(1). (152.) Id. (153.) Id. art. 18(1). (154.) Commentary on Amended Proposal, supra note 52, art. 18(1)(d). (155.) Amended Proposal, supra note 6, art. 18(2)(a). (156.) Id. art. 18(2)(b). (157.) Id. art. 18(2)(c). (158.) Id. art. 18(2)(d). (159.) Id. art. 18(2)(e). (160.) Id. art. 18(2)(f). (161.) Id. art. 18(2)(g). (162.) Commentary on Amended Proposal, supra note 52, art. 18(1)(c). (163.) Id. (164.) Amended Proposal, supra note 6, art. 19(1). Many of the smaller business that would collapse under some of the more burdensome reporting requirements would probably recieve some relief under this provision. (165.) Commentary on Amended Proposal, supra note 52, art. 19(1). (166.) Amended Proposal, supra note 6, art. 19(1). (167.) Id. art. 26(1). (168.) Id. art. 26(2). (169.) Id. In examining the legislation, both content and enforcement of general and sectoral laws must be considered. Id.; Commentary of Amended Proposal, supra note 52, art. 26. (170.) Amended Proposal, supra note 6, art. 26(1). (171.) Id. (172.) Id. (173.) Id. (174.) Id. art. 26(3); Commentary on Amended Proposal, supra note 52, art. 26. (175.) Amended Proposal, supra note 6, art. 26(3). (176.) Id. art. 26(5). This refers to international guidelines and conventions, examples of which might include the OECD Guidelines or the European Convention, both discussed above in Part II. (177.) Amended Proposal, supra note 6, art. 26(4). (178.) Id. art. 27(1). (179.) Id. art. 27(2). (180.) Id. art. 27(3). (181.) Commentary on Amended Proposal, supra note 52, art. 27. (182.) See Paige Amidon, Widening Privacy Concerns, ONLINE, July 1992, at 64,65. (183.) Cole, supra note 1, at 918. (184.) Id. (185.) Id.; see also James Kobielus, EC's New Privacy Proposals Could Hobble Global Nets, NETWORK World, Jan. 27, 1992, at 27, 27. (186.) Cole, supra note 1, at 919. (187.) Id. (188.) Id. at 920. (189.) Peter Cassidy, The Information Border Police, Info. Wk., Sept. 2, 1991, at 38, 39. (190.) Id.; see also Cole, supra note 1, at 920. (191.) Cole, supra note 1, at 920. (192.) According to a recent figure, the United States had a trade surplus of$69 billion for the services industry in 1992. John M. Berry, Forget the Trade Deficit: U.S. is aSuperpower in Services, Wash. Post, Feb 24, 1993, at D1. Moreover, the services industry is likely to become even more important in the future-nearly three-fourths of the U.S. labor force is currently employed in the service industry and nine of every 10 new jobs in the United States is in the service industry. Linda F. Powers & Frederick T. Elliot, EC 92: A Mixed Scorecard for U.S. Services Industries, Bus. Am., Feb. 25, 1991, at 16, 16. (193.) Powers & Elliot, supra note 192, at 16. (194.) See, e.g., id.; Cole, supra note 1, at 921. (195.) See Cole, supra note 1, at 921. (196.) See, e.g., id.; Powers & Elliot, supra note 192, at 16. (197.) See Cole, supra note 1, at 921. (198.) See generally id. at 920-26. (199.) Id. at 925. (200.) Id. (201.) Id. at 926. (202.) Id. at 926. (202.) Id. at 925. (203.) Id. (204.) Id. (205.) Amended Proposal, supra note 6, art. 26(1). (206.) Estadella-Yuste, supra note 34, at 175 n.22. (207.) Id. (208.) Id.; see also Reidenberg, supra note 2, at 148. (209.) See Reidenberg, supra note 2, at 153. (210.) Id. (211.) Amended Proposal, supra note 6, art. 3(1); see supra text accompanying notes 49-50. (212.) Reidenburg, supra note 2, at 153. (213.) Amended Proposal, supra note 6, art . 18(1). (214.) Estadella-Yuste, supra note 34, at 175 n.22. (215.) William L. Fishman, Introduction to Transborder Data Flows, 16 Stan. J. Int'l L. 1, 5 (1981) (216.) Id. at 5-6. (217.) Id. at 5. (218.) The beginnings of privacy rights

lie in the famous law review article on privacy by Brandeis and Warren in 1890. Id.; see Louis D. Brandeis & Samuel D. Warren, The Right to Privacy, 4 Harv. L. Rev. 193 (1890). (219.) Fishman, supra note 215, at 5. (220.) George B. Trubow, The European Harmonization of **Data Protection** Laws Threatens U.S. Participation in Trans Border Data Flow, 13 Nw. J. Int'l L. & Bus. 159, 162 (1992). (221.) Id. at 163. This law is the Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1897 (1974) (codified at 5 U.S.C. [sections] 552a (1988)). (222.) See supra text accompanying note 15. (223.) Kirby, supra note 9, at 38. (224.) Right to Financial Privacy Act of 1987, Pub. L. No. 95-630, [sub-sections] 1100-122, 92 Stat. 3697 (codified in scattered sections of 12, 31 U.S.C.). (225.) 15 U.S.C. [sub-section] 1681 (1988). (226.) Id. (227.) 20 U.S.C. [sections] 1232g(b)(2)(A)-(B) (1988). (228.) 15 U.S.C. [sections] 1666 (1988). (229.) Id. [sections] 1692. (230.) Id. [sections] 1693. (231.) See Reidenberg, supra note 2, at 149. (232.) Id. (233.) Id. (234.) See Amidon, supra note 182, at 65. (235.) See, e.g., Domestic and International **Data Protection** Issues: Hearings Before the Government Information, Justice, and Agriculture Subcomm. of the House Comm. on Government Operations, 102d Cong., 1st Sess. 14 (1991) (statement of John Baker, Senior Vice President of Equifax Inc.) [hereinafter Domestic and International Hearings]. (236.) **Data Protection** , Computers, and Changing Information Practices: Hearing Before the Government Information, Justice, and Agricultural Subcomm. of the House Comm. on Government Operations, 101st Cong., 2d Sess. 44 (1990) (summary statement of Richard A. Barton, Senior Vice President of Direct Marketing Association) [hereinafter **Data Protection** Hearings]. (237.) Id. (238.) Id. at 82 (testimony by Richard Barton). (239.) Id. at 18 (testimony by Professor David Flaherty, Professor of History and Law, University of Western Ontario). (240.) **Data Protection** Hearings, supra note 236, at 2 (opening statement by Chairman Robert E. Wise, Jr.). (241.) See supra text accompanying notes 222-34. (242.) Amidon, supra note 182, at 64. (243.) See id. at 66; Domestic and International Hearings, supra note 235, at 27 (attachment to the summary statement of John Baker, Senior Vice President of Equifax Inc.). (244.) Alan Redding Consumer Worry Halts Data Bases, Advertising Age, Feb. 11, 1991, at 28, 28; Amidon, supra note 182, at 67. (245.) This survey was completed by 126 companies in the Fortune 500. Domestic and International Hearings, supra note 235, at 99 (Research Survey of Individual Privacy Protection in Big Business). (246.) Id. at 109. (247.) **Data Protection** Hearing, supra note 136, at 2 (opening statement by Chairman Robert E. Wise, Jr.). (248.) Id. (249.) Sensitive data under the amended Proposal includes information about a person's health, sexual preferences, racial background, religious views, political views, or trade union membership. Amended proposal, supra note 6, at. 8(1). (250.) Two such organizations are the Employee Information Services in Gretna, La. and the Industrial Foundation of America in Odessa, Texas. **Data Protection** Hearing, supra note 236, at 146 (summary statement of David Czernik, Executive Director, Louisiana Consumers League). (251.) Id. at 145-46. (252.) Id. (253.) Amidon, supra note 182, at 64. (254.) Id. (255.) See Reidenberg, supra note 2, at 167-70. (256.) See id. at 172-74. (257.) Amended proposal, supra note 6, art. 16. (258.) Id.; see supra text accompanying notes 142-50. (259.) See, e.g., Cole, supra note 1, at 921. (260.) Commentary on Amended Proposal, supra note 52, art.d 16. (261.) Amended Proposal, supra note 6, art. 3 (262.) Id. (263.) Reidenberg, supra note 2, at 167-70. (264.) see Amended Proposal, supra note 6, art. 8(1); Berkvens, supra note 36 (255.) Amended Proposal, supra note 6, art. 18. (266.) Id. art. 19. (267.) Commission amends **Data Protection** Proposal, The Reuter European Community Report, Oct. 23, 1992, available in LEXIS, Europe Library, EURSCP File. (268.) Id. arts. 10, 11. (269.) Amended proposal, supra note 6, art. 26. (270.) Id.; see also supra text accompanying notes 170-73. (271.) This is less onerous than the original "opt-in" provisions of the original draft directive, under which each consumer had to give permission before any use of his or her name. Vigorous lobbying by the European Direct Marketing Association led to the change in the Amended Proposal. Chevan, supra note 89, at 49. See Amended Proposal, supra note 6, art. 15(3); Draft Directive, supr note 34, art.8(1). (272).

Chevan, supra note 89, at 49. (273). Leslie Goff, Patchwork of Laws Slows EC Data Flows, Computerworld, Apr. 13, 1992, at 80, 80. (274.) Amended Proposal, supra note 6, art. 17(1). (275.) Chevan, supra note 89, at 49. (276.) Amidon, supra note 182, at 65. (277.) See, Eg., Chevan, supra note 89, at 49. (278.) Amidon, supra note 182, at 64. (279.) See Mark B. Feldman & David R. Garcia, National Regulation of Transborder Data Flows, 7 N.C.J. Int'l L. & Com. Reg. 1, 23-25 (1982). (280.) Amended Proposal, supra note 6, art. 26(4). (281.) Estadella-Yuste, supra note 34, at 174-79. (282.) See Feldman & Garcia, supra note 279, at 24-25. (283.) See Cole, supra note 1, at 918; Cassidy, supra note 189, at 38-39. (284.) Most organizations that run communications through long distance networks must lease dedicated communication lines from the national telephone and telegraph companies to gain the bandwith and reliability needed to transmit massive amounts of information. (285.) Fishman, supra note 215, at 8-9. (286.) Feldman & Garcia, supra note 279, at 7. (288.) Reidenberg, supra note 2, at 140. (289.) GATT and Services: Second Best, Economist, Aug. 3, 1991, at 62, 64. (290.) Council of Ministers: Consumer Legislation Up for Debate on November 11 an 19, Europe Environment, Nov. 9, 1993, available in LEXIS, Nexis Library, OMNI File. (291.) **Data Protection** : Agreement Now Likely Before the End of the Year, Europe Environment, Oct. 1 1993, Available in LEXIS, Nexis Library, OMNI File. (292.). Id.

INDUSTRY CODES/NAMES: GOVT Government and Law; INTL Business, International
DESCRIPTORS: Information law--International aspects; Computers--Access control; Confidential communications--Laws, regulations, etc.
GEOGRAPHIC CODES: ZEEC; NNUS
FILE SEGMENT: LRI File 150
?

? t s9/full/3

9/9/3 (Item 3 from file: 15)
DIALOG(R)File 15:ABI/INFORM(R)

01208644 98-58039

Legal lessons in the computer age

Rasch, Mark D

Security Management v40n4 PP: 59-67 Apr 1996 ISSN: 0145-9406
JRNL CODE: SEM
DOC TYPE: Journal article LANGUAGE: English LENGTH: 6 Pages
WORD COUNT: 4545

ABSTRACT: Computers and computer networks create new categories of crimes that did not exist in the precomputer age. For example, files may be stolen even though the owner still retains copies. Money may be siphoned using so-called salami-frauds or round-down frauds where hundredths of a cent may be shaved off millions of transactions. Private information may be intercepted through interference with e-mail. Services, including the simple use of computers and computer networks, may be usurped by ingenious hackers. While technology has advanced quickly, the law has not. New crimes often do not fit parameters of the preexisting legal framework. Since 1982, Congress has attempted to craft new statutes covering computer crime. Those efforts have helped, but gaps remain. Companies hoping to protect their systems and information, while also avoiding inadvertent violations of the law themselves, face the challenge of working within this confusing and evolving legal framework. This issue is addressed in detail.

TEXT: Headnote: Computer technology has changed the nature of crime. And now legislatures and the courts are racing to catch up.

Computers and computer networks create new categories of crimes that did not exist in the precomputer age. For example, files may be stolen even though the owner still retains copies. Money may be siphoned using so-called "salamifrauds" or "round-down" frauds where hundredths of a cent may be shaved off millions of transactions. Private information may be intercepted through interference with e-mail. Services, including the simple use of computers and computer networks, may be usurped by ingenious hackers.

While technology has advanced quickly, the law has not. New crimes often do not fit the parameters of the preexisting legal framework.

Since 1982, Congress has attempted to craft new statutes covering computer crime. Those efforts have helped, but gaps remain. As new cases make their way through the legal system, some of these gaps are being filled in by precedent setting decisions. Companies hoping to protect their systems and information, while also avoiding inadvertent violations of the law themselves, face the challenge of working within this confusing and evolving legal framework.

Current law. The first truly comprehensive federal computer crime statute was the Computer Fraud and Abuse Act of 1986 (CFAA). The statute was the rewritten version of a 1984 statute that proved inadequate in dealing with the problem of computer crime.

The act amended Title 18 United States Code 1030 to enhance penalties for six types of computer activities: the **unauthorized** access of a computer to obtain information of national secrecy with an intent to injure the United States or give advantage to a foreign nation; the **unauthorized** access of a computer to obtain protected financial or credit information; the **unauthorized** access into a computer used by the federal government;

the **unauthorized** interstate or foreign access of a computer system with an intent to defraud; the **unauthorized** interstate or foreign access of computer systems that results in at least $1,000 aggregate damage; and the fraudulent trafficking in computer passwords affecting interstate commerce.

Perhaps the most famous application of this statute was United States v. Morris (Second Circuit, 1991), the 1989 prosecution of Robert Tappan Morris, a Cornell University graduate student who, on November 2, 1988, released a computer "worm" across the Internet computer network.

Despite the successful prosecution in the Morris case and several other famous computer crime prosecutions (including prosecutions of computer hackers of the Legion of Doom and Masters of Deception), problems continued with the statute. The most glaring was the omission of what was called malicious codecomputer viruses that could alter, damage, or destroy computerized information.

As a result, in 1992 Congress amended the computer crime statute to punish those who, without the knowledge and authorization of the "persons or entities who own or are responsible for" a computer, bring about the transmission of "a program, information, code, or command to a computer or computer system" with the intent to cause damage to the computer or information in the computer or prevent the use of the system.

As well as punishing intentional conduct, the amended statute criminalizes those who act "with reckless disregard or a substantial and unjustifiable risk" of damage or loss, and would create a civil cause of action to obtain compensatory damages or injunctive relief for "any person who suffers damage or loss by reason of a violation of the section."
In addition to **protecting** the **data** contained on computers, federal law also attempts to protect the integrity or confidentiality of electronic communications-either during transmission or while **stored** . Section 2701 protects e-mail messages by making it illegal to destroy e-mail messages or access them without authorization.

In addition, in 1986 Congress amended the federal wiretap law, passing the Electronic Communications Privacy Act (ECPA) to expand federal jurisdiction and to criminalize the **unauthorized** "interception" of stored and transmitted electronic communications. The statute makes it unlawful to either intercept or disclose the contents of electronic communications, except as provided by statute. Thus, capturing or monitoring the contents of e-mail messages, electronic communications, or stored electronic communications may violate these provisions.

The law does permit providers of telecommunications facilities to engage in some monitoring for the protection of those facilities. In addition, the law allows monitoring if at least one of the parties to the monitoring has consented. Thus many companies use warning banners to notify users of their intent to monitor electronic mail, creating an implied consent.

The Justice Department's Computer Crime Unit, in conjunction with a number of federal agencies known as the Computer Search and Seizure Working Group, have developed guidelines to address seizing computers and handling computer evidence. (See "Legal Reporter," May 1995)

The guidelines run several hundred pages, addressing the many scenarios under which government officials could, in connection with criminal investigations, search or seize a company's (or a person's) computer data or equipment-including everything from computer hardware to e-mail messages.

Additional computer crime provisions have been included in the Senate crime bill, S. 1495, and in the National Information Infrastructure Act, S. 982. If enacted, these measures would increase penalties for computer crime and include harassment through computer communications as a computer crime. S.

982 would also expand the scope of the federal computer crime statute to criminalize **unauthorized** access to all information contained in a computer. However, it is unclear whether these bills-which have been stalled in committee-will pass during this congressional session.

Evolving precedents. Where new laws have not kept up with the changing face of crime, **authorities** have used traditional statutes-mail and wire fraud, larceny, theft of services, embezzlement, trespass, and destruction of property-to prosecute individuals who commit forms of computer abuse. Because these laws were not written with computer crimes in mind, courts must carve out new precedents.

Information. The application of common law concepts of fraud, theft, and trespass were an ill fit to the new technology that emerged in the late 1960s. For example, the federal embezzlement statute (18 U.S.C. 641) proscribes the "conversion" or taking for one's own purposes of federal property. (There is no federal statute relating to the taking of commercial property). But it was unclear from the statute 's inception whether information contained on a computer was truly property subject to conversion. The computer crime law of 1986, as already discussed, carved out certain circumstances under which the tampering with or taking of computer information would be a crime, but it did not establish a blanket protection for digitized information.

While some early cases, such as Chappel v. United States (Ninth Circuit,1959), held that the embezzlement statute applies only to "corporeal or tangible property," most courts have ruled in the opposite direction. Convictions have been upheld for **unauthorized** use of computer time, theft of grand jury transcripts, and photocopying government records. Most recently, in United States v. McAusland (Fourth Circuit, 1992), an employee was convicted of embezzlement for stealing a competitor's confidential bid information. The defendant, an employee of a defense contractor, obtained bid information by working with an employee at a competing company. The defendant was convicted of conspiracy to embezzle. While computer and computer information were not used in the crime, the case set the groundwork for determining whether information can be considered property.

Other difficulties arise in the prosecution of individuals for the theft of information. For example, the crime of theft or larceny, according to common law, requires proof of "asportation" or the "taking away" of the property. In the instance of theft of computerized information, the stolen property may remain precisely where it was, and the owner may not be deprived of its use.

Similarly, concepts of trespass and breaking and entering do not fit well into the electronic environment. There is no physical entry into the computer, and therefore, no common-law trespass.

Prosecutors have attempted to base charges on provisions of the wire fraud statutes, again with mixed results. For example, in United States v. Riggs (Northern District of Illinois, 1990), defendants Robert Riggs and Craig Niedorf, admitted computer hackers, devised what the district court accepted to be a scheme to steal software and other intellectual property belonging to Bell South. The data was designed to regulate the company's enhanced 911 (E911) emergency call system.

Riggs accessed the Bell South computer using other people's passwords and downloaded a text file that described the system. Though theoretically the pair could have been convicted under the wire fraud statute for stealing passwords, the two were never charged with this crime. Instead, the case concentrated on whether the information stolen could be considered property. The attorneys for the defense argued that the E911 data did not constitute property and that, therefore, no crime was committed.

In this instance, the court shared the prosecutor's view that the old law could be adapted to address the new crime. The district court, in denying the motion to dismiss the wire fraud count, observed: "... the object of the defendants' scheme was the E911 text file, which Bell South considered to be valuable, proprietary information. The law is clear that such valuable, confidential information is 'property,' the deprivation of which can form the basis of a wire fraud charge."

Other courts have come to the opposite conclusion. For example, United States v. LaMacchia (District of Massachusetts, 1994) involved a twentyone-year-old student (David LaMacchia) at the Massachusetts Institute of Technology who had created an electronic bulletin board on the Internet that was accessible to anyone. He actively encouraged correspondents to upload copyrighted commercial software, which he then posted to another bulletin board for download by others.

Because he made no money from this endeavor, LaMacchia could not be charged with criminal copyright violations. (The case is distinct from civil copyright cases, which require no evidence of economic benefit.) Instead, he was indicted for one count of conspiring to commit wire fraud. According to the indictment, he was facilitating the illegal copying and distribution of copyrighted software without payment of licensing fees and royalties to software manufacturers and vendors.

The district court, relying in large measure on the Supreme Court's holding in Dowling v. United States, 473 U.S. 207 (1985), took the unusual step of dismissing the wire fraud indictment prior to trial. In Dowling, the Supreme Court reversed a defendant's conviction for interstate transportation of stolen property. That case had involved the shipping of pirated Elvis Presley recordings across state lines **without permission** and without the payment of royalties to the copyright holder.
The Dowling court found that while a criminal copyright violation may have occurred in that case (because the transportation of the recordings was for profit), no violation of the statute could be found because the property transported across state lines-the recordings-was not truly stolen. The Supreme Court suggested that the recordings, while evidence of potential copyright violations, were not property "taken" by fraud.

In LaMacchia, the district court observed that the dismissal of the fraud indictment was mandated by the ruling in Dowling because of the fundamental difference between intellectual property and tangible property.

In another case, United States v. Brown (Tenth Circuit, 1991), the circuit court, also relying on Dowling, reversed the defendant's conviction for stealing a source code created by his former employer. The defendant had downloaded a copy of the source code onto his home computer, which was discovered later when a search was conducted in accordance with a warrant. This is not prosecutable under the Computer Fraud and Abuse Statute because it did not involve **unauthorized** entry. Dowling used his old password, which had not been purged from the computer system, to obtain the data.

In dismissing the indictment, the court observed that "Dowling holds that the statute applies only to physical goods, wares, or merchandise. Purely intellectual property is not within this category. It can be represented physically, such as through writing on a page, but the underlying, intellectual property itself, remains intangible."

While deprived of criminal remedies, companies can still pursue civil cases. The intent behind the law is to protect those that, for example, download copyrighted material to read later. It also makes these types of copying distinct from those taking material to resell it or gain other economic benefit.

The bills pending before Congress would expand the definition of economic benefit to include the bartering of software. Such a law might have

criminalized LaMacchia's conduct.

Trade secrets. Various states have statutes that criminally punish the theft or misappropriation of trade secrets. But charges would only be appropriate under this law if the prosecutor could demonstrate that the information at issue was a trade secret and that the owner of the property and the defendant had entered into an agreement restricting rights to the information that was taken.

Trade secret case law in the computer age was established in the 1970s in cases where employees were convicted under state trade secret laws for downloading and printing an employer's proprietary software.

Where the offender is not an insider, a trade secret prosecution is not an option. Furthermore, while the misuse of a trade secret, like the misuse for profit of copyrighted information, may constitute a criminal offense, the mere possession of a trade secret or its misappropriation may not constitute a crime.

A recent case typifies the problem of the enforcement of trade secrets in cyberspace. In Religious Technology Center v. Netcom et al (Northern District of California, 1995), the court declined to continue an injunction preventing the further publication of the trade secrets of the Church of Scientology.

One of the defendants in the case had obtained what the court concluded were secret internal documents of the church and had posted them on various Internet newsgroups. The defendant asserted that he had received some of the documents from various anonymous, publicly accessible Internet sites. The court concluded that information posted to the Internet could no longer be considered secret. Therefore, the individual who obtained the information from a public domain could not be held responsible for theft of trade secrets.

Further, the court ruled that "...evidence that another individual has put the alleged trade secrets into the public domain prevents the plaintiff from further enforcing its trade secret rights to those materials."(In a copyright case involving the same incident, a court ruled that copyrights still apply to material on the Internet.)

Privacy. In Steven Jackson Games Inc., v. United States Secret Service (Fifth Circuit, 1994), the court held that the seizure of a computer containing unread e-mail is not an unlawful intercept under the Electronic Communications Privacy Act.

Steven Jackson Games, Inc., (SJG)-a publisher of books, magazines, and computer games-operated a bulletin board system that was accessible to SJG employees, customers, and freelance writers. One of SJG's employees was implicated in a scheme to steal proprietary information. As a result, the federal government seized SJG's computers, including unread email messages. SJG sued the Secret Service for violation of the Privacy Protection Act and the Electronic Communications Privacy Act-under which it is illegal to intercept electronic communications but legal for government officials to view stored electronic communications after obtaining a warrant.
Because the Secret Service obtained a warrant to search the property but not to seize computer information, the appeals court awarded damages to SJG. However, the court also ruled that the Secret Service did not violate the first provision of the ECPA because the email communications on the computer were not intercepted while they were being transmitted.

Services. It is clear that computer time, in appropriate circumstances, constitutes a thing of value. Computers and computer networks are expensive machines and cost time and money to establish and maintain. However, the **unauthorized** use of computer time does not always deprive the owner of the use of his or her computer.

Efforts to apply theft statutes to the theft of computer services have met with mixed success. In several cases tried in the late 1970s, the courts found that **unauthorized** use of computer time did not constitute a crime. Since then, the court decisions have shifted. Some courts have found employees guilty of mail fraud and embezzlement for using computers for personal business.

In Lund v. Commonwealth (Virginia, 1977), the court refused to find an offense in the **unauthorized** use of a computer. Likewise, in State v. McGraw (Indiana, 1985), the court found that an employee's computer use did not deprive the owner of the ability to use the computer system, nor did it constitute a theft of services. In United States v. Sampson (Northern District of California, 1978), the court found that **unauthorized** use of computer time constituted embezzlement, and in United States v. Kelly (Eastern District of Pennsylvania, 1981), an employee was convicted for mail fraud because computer time used for private means was considered a scheme to deprive the employer of services.

Most recently, the Arizona Court of Appeals has added another twist in Re Commodore Computers, 804 P.2d 100 (Arizona Appeals Court, 1991), finding that state and federal crime statutes were not sufficient to judge whether the defendant had used the computer to gain **unauthorized** access into his employer's computer system. A long distance telephone company had noticed repeated attempts to break into its computer system. An investigation found that the attacks were coming from a telephone company employee's personal computer.

The court ruled that such evidence did not prove that the person attempted to gain **unauthorized** access. In addition, the court ruled that the seizure of the employee's computer was **unauthorized** under the Arizona computer crimes act. The act states that a computer cannot be forfeited due to an attempted computer break-in.
Property destruction. Another offense complicated by the nature of computers is the destruction of property. If an offender equipped with a sledge hammer pummels a computer into an unrecognizable pile of chips and wires, he or she has clearly committed the offense of destruction of property. If the same offender, equipped with a modem, deletes files from a computer system, all he or she has done is to change the polarity of a magnetic medium, which may or may not constitute a destruction of property.

While Congress attempted to address this concern with the Computer Fraud and Abuse law, it does not clearly define the concept of "loss." If information is stolen from a company, but the data still resides on the organization's computer system, it is unclear whether a loss has occurred.

The federal statute, rather than address destruction of property, addresses the concept of loss through **unauthorized** access, leaving open the question of whether computerized information is property and whether theft or deletion of the information is destruction of that property.

Companies may find their level of legal recourse for such destructive actions varies depending on the state in which the crime occurs. Texas, for example, adapted its legal code to criminalize **unauthorized** conduct that causes a computer to malfunction or that destroys or alters computer data. In Burleson v. Texas (Texas Appeals Court, 1991), Burleson, a senior programmer, was fired. In retaliation, he inserted into the company's computer system a software program called a logic bomb. The program was designed to delete files responsible for calculating payroll commissions for more than 400 employees.

In this case, the crime was committed in a state that had brought its laws up to date. He was successfully prosecuted for violation of the Texas computer crime statute, passed in 1985 and updated in 1989, which makes it

a crime for anyone to knowingly cause a computer to malfunction without the authorization of the owner or to alter, damage, or destroy data or programs without the consent of the owner.

The court's ruling illustrates that the insertion of software devices designed to disable computer systems without the authorization of the owner may subject the perpetrator to both civil and criminal liability.

Jurisdiction. As the previous section illustrates, some crimes have traditionally been handled at the state level, and states are adapting their legal framework with computer-related laws, but one of the biggest problems with applying traditional criminal law concepts to cyberspace is the difficulty of establishing jurisdiction and venue.
The law defines most crimes as having occurred either where the defendant committed the act or where the victim of the offense was located. Unfortunately, cyberspace has no clear location or boundaries. A user may be at one location, the computer in a second location, and the offending message or resulting act caused by software may occur in a third or in multiple locations.

Defamatory, malicious, or pornographic messages posted on the Internet are globally accessible. From a business perspective, this can cause problems for a company that is trying to hold a troublemaker accountable. It can also cause trouble for a company that unwittingly exposes itself to charges of wrongdoing on the Internet. That can occur because, by accessing the Internet, users may unintentionally find themselves subject to local jurisdictions at the other end of the network. Courts are only just beginning to wrestle with this issue.

A recent prosecution in Tennessee, United States v. Thomas (Sixth Circuit, 1996), illustrates the problem of jurisdiction in cyberspace. In 1994, Robert and Carleen Thomas, a couple living in San Francisco, were indicted by a federal grand jury in the Western District of Tennessee for operating a computer bulletin board that contained what the federal government considered obscene and pornographic photographs available for downloading by the general public. Prior to the indictment, police in Milpitas, California, conducted a search and found that the files did not violate the "contemporary community standards" of the San Francisco area and were, therefore, not legally obscene. The Thomases appealed the district court's decision.

On January 29, 1996, the Sixth Circuit affirmed the lower court's decision. The court ruled that, unlike the Internet, bulletin boards are under the control of the operator. Therefore, when a subscriber from Memphis, Tennessee, logged onto the Thomases' bulletin board, the couple agreed to abide by the community standard of Memphis.

State statutes. Every state except Vermont has enacted a computer crime statute. Many of these are based on the federal Computer Fraud and Abuse Act of 1986 referenced earlier, but they vary widely in their definitions of computers, computer systems, computer networks, computer supplies, data, and other fundamental terms.

Recently, state legislatures have grappled with the issue of computer crime as has the federal government. States have met these challenges with varying degrees of success. New York is considered a fairly typical representation of how states are handling computer crimes.
According to Lance Rose-who discusses crimes and online services in his book Netlaw: Your Rights in the Online World-New York first enacted a computer crimes statute in 1986 and amended it in 1992. The New York provision covers several kinds of computer crimes including **unauthorized** use, computer trespass, computer tampering, duplication of computer-related material, and criminal possession of computer-related material.

Unauthorized use. **Unauthorized** use is a misdemeanor and the least

serious of the New York computer crime offenses. It is designed to thwart the curious hacker who gains entry into another's computer system to look around rather than to do damage.

Computer trespass. To be deemed guilty of computer trespass, a user must gain **unauthorized** access to a computer system and then either commit a felony or obtain "computer material," which is narrowly defined under the New York law as protected commercial information available only to specified members of the company. Examples of computer material include trade secrets, databases, and member lists. Information available to the public by computer or other means cannot be considered computer material.

Computer tampering. As redefined by the 1992 amendment to the computer crime statute, computer tampering includes four levels. First degree tampering, a misdemeanor, includes knowingly reformatting a system or deleting files. (The tampering provision does not apply if the information deleted is computer material. Such crimes would be prosecuted under the computer trespass section of the statute.)

Second, third, and fourth degree tampering are felonies. The severity of the felony increases as the nature of the crime-and damage caused-becomes more serious. To commit a computer tampering felony, a user must meet one of the following criteria:

* Commit a felony in the course of tampering with a computer system

* Be a former felon, convicted of previous computer crimes

* Intentionally alter or destroy computer material

* Intentionally alter or destroy computer data or programs at a cost exceeding $1,000

Duplication of computer material. Also a felony, duplication of computerrelated material refers to the copying of computer data **without permission** , where the copier reaps an economic benefit of at least $2,500. The statute also makes it a felony to copy computer data while committing a felony.

New York has experienced some difficulty upholding this aspect of the statute because of a conflict with federal law. The U.S. Copyright Act forbids states to pass laws that make copying illegal.

Various bills pending before Congress would, if passed, expand the scope of federal copyright protection for digital information. One such bill, S. 1284, would adapt existing copyright law to apply to documents and materials in electronic format. The proposed legislation also prohibits the use, importation, manufacture, or distribution of any device that would disable or prevent the inclusion of copyright information on a document.

Criminal possession of computer material. This provision makes it illegal to possess illegally copied computer data or programs knowingly. This language allows the state to prosecute an accomplice who is merely "holding" the data stolen by someone else; however, this aspect of the statute also conflicts with federal copyright law.

Other aspects of the statute have been tested in court. The computer tampering provision was upheld in The People v. Robert Versaggi (Rochester City Court, 1987). Versaggi was employed by the Eastman Kodak Corporation as a computer technician and was responsible for the maintenance and repair of several telephone systems. Versaggi was charged with computer tampering that disrupted and disconnected Kodak's telephone system on several occasions.

The defense argued that Versaggi was not guilty of altering Kodak's

computer system because the features activated by Versaggi were existing features of the program. The defense argued that altering should be defined as adding or creating a destructive program, not activating an existing one.

The prosecution contended that Versaggi's action should be considered tampering because he intentionally interrupted telephone service by overriding existing computer commands.

Versaggi was convicted of computer tampering by the Rochester City Court in 1987. The case was affirmed by the New York State Court of Appeals in 1994.

This snapshot of current law and court rulings gives security professionals a glimpse into the evolving legal landscape that companies must be prepared to negotiate when pursuing those who might attempt to steal or damage computerized systems or information. Understanding what is criminal at the state and federal level and how the law views computerized assets is an important first step toward establishing good internal protection policies.

Author Affiliation: Mark D. Rasch, J.D., is the director of information security law and policy at the Center for Information Protection at Science Applications International Corporation in McLean, Virginia, a commercial information security consulting company. He is a frequent writer and speaker on computer crime, and headed the Department of Justice's computer crime efforts until 1991. He was responsible for prosecuting Robert Tappan Morris, the first use of the federal computer crime statute.

GEOGRAPHIC NAMES: US

DESCRIPTORS: Computer security; Computer crime; Legislation; Litigation
CLASSIFICATION CODES: 9190 (CN=United States); 5140 (CN=Security); 4300 (CN=Law)
?

09/000924 priority 6/11/97

? *show files, ds*

File 2:INSPEC 1969-2000/Jan W5
(c) 2000 Institution of Electrical Engineers
File 6:NTIS 64-2000/Mar W4
Comp&distr 1998 NTIS, Intl Copyright All Righ
File 8:Ei Compendex(R) 1970-2000/Feb W1
(c) 2000 Engineering Info. Inc.
File 9:Business & Industry(R) Jul/1994-2000/Mar 09
(c) 2000 Resp. DB Svcs.
File 15:ABI/INFORM(R) 1971-2000/Mar 08
(c) 2000 Bell & Howell
File 16:Gale Group PROMT(R) 1990-2000/Mar 09
(c) 2000 The Gale Group
File 34:SciSearch(R) Cited Ref Sci 1990-2000/Feb W4
(c) 2000 Inst for Sci Info
File 35:DISSERTATION ABSTRACTS ONLINE 1861-1999/DEC
(c) 2000 UMI
File 65:Inside Conferences 1993-2000/May W4
(c) 2000 BLDSC all rts. reserv.
File 77:CONFERENCE PAPERS INDEX 1973-2000/JAN
(c) 2000 CAMBRIDGE SCI ABS
File 94:JICST-EPlus 1985-2000/Nov W2
(c)2000 Japan Science and Tech Corp(JST)
File 98:General Sci Abs/Full-Text 1984-1999/Oct
(c) 1999 The HW Wilson Co.
File 99:Wilson Appl. Sci & Tech Abs 1983-2000/Jan
(c) 2000 The HW Wilson Co.
File 144:Pascal 1973-2000/Feb
(c) 2000 INIST/CNRS
File 148:Gale Group Trade & Industry DB 1976-2000/Mar 08
(c)2000 The Gale Group
File 233:Internet & Personal Comp. Abs. 1981-2000/Mar
(c) 2000 Info. Today Inc.
File 238:Abs. in New Tech & Eng. 1981-2000/Feb
(c) 2000 Reed-Elsevier (UK) Ltd.
File 239:Mathsci(R) 1940-2000/Feb
(c) 2000 American Mathematical Society
File 256:SoftBase:Reviews,Companies&Prods. 85-2000/Feb
(c)2000 Info.Sources Inc
File 278:Microcomputer Software Guide 2000/Jan
(c) 2000 Reed Elsevier Inc.
File 266:FEDRIP 2000/Feb
Comp & dist by NTIS, Intl Copyright All Rights Res
File 275:Gale Group Computer DB(TM) 1983-2000/Mar 09
(c) 2000 The Gale Group
>>>Invalid SHOW option: ,
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
(c) 1998 Inst for Sci Info
File 553:Wilson Bus. Abs. FullText 1982-1999/Sep
(c) 1999 The HW Wilson Co
File 621:Gale Group New Prod.Annou.(R) 1985-2000/Mar 09
(c) 2000 The Gale Group
File 624:McGraw-Hill Publications 1985-2000/Mar 09
(c) 2000 McGraw-Hill Co. Inc
File 636:Gale Group Newsletter DB(TM) 1987-2000/Mar 09
(c) 2000 The Gale Group
File 647:CMP Computer Fulltext 1988-2000/Feb W4
(c) 2000 CMP
File 674:Computer News Fulltext 1989-2000/Feb W3
(c) 2000 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2000/Mar 08
(c) 2000 The Dialog Corp.
?

```
? ds

Set     Items   Description
S1          0   (INPUT?3 OR STOR?3) (S) (PROTECT?3 (5N) DATA)
S2      11542   (INPUT??? OR STOR???) (S) (PROTECT??? (5N) DATA)
S3      11447   S2 NOT PD>=06111997
S4      11447   S2 NOT PD=>06111997
S5       6951   S2 NOT PY>1997
S6       6100   S5 AND (PROTECT??? (3N) DATA)
S7          0   S6 AND (??AUTHORI????)
S8        928   S6 AND (AUTHORI????? OR UNAUTHORI?????)
S9          9   S8 AND (WITHOUT (W) PERMISSION?)
?
```

(consider all)

? *t s9/full/6*

9/9/6 (Item 3 from file: 148)

04812991 SUPPLIER NUMBER: 09408681 (THIS IS THE FULL TEXT)
Employee dishonesty and workplace security: precautions about prevention.
Kandel, William L.
Employee Relations Law Journal, 16, n2, 217-231
Autumn, 1990
ISSN: 0098-8898 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 6632 LINE COUNT: 00561

TEXT:

This column is the second in a two-part series focusing on employee dishonesty and workplace security. Part I outlined several statutory and common law risks to which employers are exposed when they implement preventive or punitive measures to reduce employee dishonesty. Among those risks, the potential for defamation claims has recently increased: The notion that expressions of "opinion" that imply a false assertion of fact nonetheless enjoy a First Amendment exemption from application of state defamation laws was dispelled by the United States Supreme Court in Milkovich v. Lorain Journal Co., 58 U.S.L.W. 4846 (U.S. June 21,1990) (No. 89-645).

This columnm continues the overview of issues associated with employee dishonesty and offers suggestions to employers for effective security measures that will not infringe on employees' rights. Preserving Trade Secrets

The competitive harm from disclosure of proprietary information should motivate prudent employers to undertake an affirmative program of loss prevention. The free flow of ideas has its limits, particularly when the subject is "trade secrets." A trade secret has been defined as "a formula, pattern, device, or compilation of information that is used in one's business and that gives one the opportunity to obtain advantage over competitors who do not know or use it. A plan or process, tool, mechanism, or compound known only to its owner and those of his employees to whom it is necessary to confide it."[1] A more action-oriented definition is contained in Section 1(4) of the Uniform Trade Secrets Act:

Trade secret means information including a formula, pattern, compilation, program, device, method, technique or process that (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[2]

Even these definitions of trade secret are too restrictive, however. As any employer in a competitive business knows, a variety of encroachments on intellectual property can cause competitive harm. Thus, to learn the competitor's confidential plans for marketing, growth, profitability, or new products is to gain an advantage, as is access to the competitor's confidential lists of customers, suppliers, or distributors. For example, government contractors frequently oppose public disclosure of employment-related bid data in fear that competitors will be able to extrapolate material costs and profit margins. Employers have competitive reasons, among others, to maintain the secrecy of turnover, morale, and related conditions of key employees.

Not all of this confidential information may be shielded. Patent and copyright laws go only so far and are beyond the scope of this discussion. Trade secret protection varies according to state law, but still allows some degree of generalization. Trade secrets have been stolen by employees with impunity when the employer failed to back up with action its subjective belief that the information was a valuable secret. It is not always self-evident to employee-or courts and juries-that specific

information deserves protection. The law requires employers to act on their belief that a trade secret exists by proclaiming, promulgating, and protecting.

Thus, the first step in preventing loss of intellectual property is to establish that the information is indeed secret by communicating this fact in such a manner that everyone understands, especially employees and possible judges or juries, and by taking steps to maintain confidentiality and nondisclosure so that the secret's protection is not lost or inadvertently waived. The second step is to make clear that employees who receive trade secrets are obligated to protect them and to obtain written commitment from employees that they will maintain the confidentiality of these secrets. Employers thus establish grounds under state common law, even when fiduciary obligations are uncertain, to hold liable any employee who breaches the contractual duty of confidentiality.

Employers are surprisingly lax about establishing programs to protect trade secrets. Even in high-tech industries, where secrecy has the highest competitive value, a recent survey of trade secret theft revealed that 34 percent of responding companies had no protective program.[3] Such employers are in danger of forfeiting their right to protect their trade secrets. Courts are unsympathetic to belated secrecy claims by employers that have not bothered previously to guard that information. Thus, the survival of one's right to protect trade secrets is almost Darwinian: use it or lose it.

Programs that protect proprietary information among employees must include clear written policies and procedures, augmented by ongoing dissemination and training. From orientation of new employees through exit interviews of departing employees, this trade secret policy must be reiterated. Oral presentation alone is insufficient; documentation must memorialize these communications, along with employee signatures acknowledging their receipt. This is not merely a papertrail exercise for litigation purposes, but is traditional personnel management, that is, documentation to facilitate audit and control. A reason to assume this burden is that accidental disclosure of trade secrets can be devastating, a risk reducible by an affirmative program.

In addition to establishing a climate of confidentiality, the conscientious employer should take practical steps geared to the particular secrets to be protected. The paperwork boom in most businesses and industries makes document control central to security programs. From production to destruction, documents that contain elements of trade secrets must be kept from **unauthorized** eyes through precautions that are themselves documented. Written instructions may be necessary for keeping papers from open view, locking certain file cabinets, and stamping documents as confidential. Limits of employee access to company information in computer systems should be spelled out and monitored. Although many employees may be involved in aspects of a trade secret, careful employers restrict individual access on a need-to-know basis so that nobody learns more than what is absolutely necessary.

Employers should avoid a blunderbuss approach that inappropriately seeks to characterize even nonconfidential information as a trade secret. Employers that sweep too broadly risk diluting and defeating their otherwise bona fide trade secret claims. Under the best legal circumstances, it is difficult for employers to proceed successfully against former employees who disclose: The law prohibits their disclosure of specific trade secrets, but allows employees to use general skills, knowledge, experience, and ideas learned with the previous employer. Thus, specificity of trade secrets may be lost by marking too many documents as confidential, making it difficult for the employer to prove the true extent of proprietary information.

Substantial protection may be obtained through agreements signed by employees that they will neither disclose nor assign rights to the employer' s intellectual property. By requiring new hires and incumbents to undertake such obligations as a condition of employment, the employer accomplishes at least three things: (1) adding an incentive for the maintenance of trade secrets; (2) adding a contractual cause of action in the event of a disclosure; and (3) educating employees, through definitions

in the agreement, as to the scope of the employer's intellectual property. Such agreements should emphasize that these employer protections include not only what has been learned by or revealed to the employee but also any information developed by the employee. Employees should be made aware that these nondisclosure obligations extend beyond the term of employment.

Confidentiality agreements are critical in restraining key employees who develop valuable intellectual property for the employer. A legal distinction is usually made between a departing employee who has learned the employer's trade secret and an employee who actually used his or her own skills to develop the trade secret. According to the courts, absent a written confidentiality agreement, the developing employee has the right to use and disclose a trade secret.[4]

The purpose of covenants not to disclose intellectual property is primarily preventive. Employers do not require nondisclosure agreements as litigation tools. Indeed, one of the risks of litigation with employees is the disclosure of the very information that the agreement was intended to protect. Antitrust counterclaims also are a risk. By warning and educating employees, the chances of disclosures-purposeful or inadvertent-are reduced.

Preventing Computer Theft

Employers and legislators struggle to prevent technologically sophisticated employees from stealing via the computer. The difficulty in dealing with hackers was recently illustrated by the inapplicability of the federal sentencing guidelines to the first conviction under the Federal Computer Fraud and Abuse Act of 1986.[5] Neither the federal court nor the prosecutor could propose a traditional response to the crimes of Robert Morris, the computer science student convicted of writing and entering the program that halted the Internet computer network. Although his tampering cost millions of users at corporations, universities, and military sites nationwide the use of their computers, Morris did not receive the 21-27 months' prison sentence suggested by the federal guidelines.

It remains to be seen whether the Morris case will deter employees and others who may see such tampering as a game. In fact, the stakes can be enormous. For example, bank employees have diverted to their own accounts fractions of pennies of accrued interest that, in the aggregate, total hundreds of thousands of dollars. These types of offenses are now addressed in the Federal Computer Fraud and Abuse Act. In other instances, disgruntled employees have destroyed valuable computer data and planted "time bombs," "worms," and viruses" designed to erase programs or alter data when triggered by specified events.[6] One employee developed a program to delete his own personnel records, triggered by an entry indicating his employment would be terminated. The proposed Computer Virus Eradication Act would make such conduct a federal crime. Currently, only five states appear to make the introduction of computer viruses a crime.[7]

Employees have used proprietary software or business data for personal advantage, and in other cases, have sold access codes to others who could then pirate or adulterate data.[8] A less dramatic but more familiar scenario is employee use of office computer time and facilities for nonwork purposes or taking software for home computer use. When employees have made extensive **unauthorized** and concealed use of their employer's computer facilities for noncompeting personal business ventures, courts have found evidence of an intent to defraud the employer.[9]

Because of the delayed response of legislatures to computer crimes, prosecutions were initially confined to myriad state statutes not designed for such issues, often with unsatisfactory results. In Ward v. Superior Court, 3 Comp. Law Serv. Rep. 208 (1972), for example, theft of a competitor's computer program was unsuccessfully prosecuted because the electronic impulses of the computer were not "tangible property" as required by California's theft statute. Similarly, in State v. McGraw, 480 N.E.2d 552 (Ind. 1985), the Indiana Supreme Court threw out the theft conviction of a city employee who had maintained the business records of a private business on his employer's computer. Because nothing was actually taken from the employer, the prerequisite deprivation of property was lacking.

At the federal level, prosecutors have applied numerous statutes to

fill legislative gaps regarding computer crimes. Relevant federal statutes have included those regulating mail, wire and bank fraud, theft, false entries or alterations of business or public records, disclosure of confidential information, wiretapping, and interstate transportation of stolen goods. Some successful prosecutions have been fortuitous. In United States v. Giovengo, 637 F.2d 941 (3d Cir. 1980), a defendant who altered customer airline tickets and siphoned off part of the purchase price was prosecuted under the federal wire fraud statute because the computer that generated the tickets had interstate telephone accessibility.

And in United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978), cert. denied, 441 U.S. 922 (1979), a defendant who obtained a confidential program from his former employer's computer was convicted of wire fraud because the computer's wire transmissions crossed state lines. However, because nothing tangible was taken, Seidlitz was acquitted under the statute prohibiting interstate transportation of stolen property.

Despite such results, by 1986 fewer than half the states had computer crime-related statutes, and federal legislation was very narrow. Since then, computer crime statutes have been enacted by all the states, but these laws vary widely in prohibited conduct, dollar thresholds, and penalties imposed. As a recent summary of state statutes shows, forty-one states prohibit **unauthorized** access; thirty-five prohibit theft, taking, or copying of computer data; thirty-four prohibit schemes to defraud or obtain money, property, or services; and ten prohibit obtaining personal or confidential information.[10]

California's computer crime statute, the most comprehensive among the states, prohibits knowing access, or causing access **without permission** , to a computer system

(1) to defraud or wrongfully obtain money, property, or data (including copies of software, codes, and supporting documentation); (2) to obtain or make use of computerized information or systems, including using computer time or data processing; (3) to add, alter, delete, damage, or destroy computer data, software, or programs; or (4) to disrupt service or deny access to service by an **authorized** user.[11]

Comprehensive as it is, the California computer crime statute nonetheless exempts employees if they were acting within the scope of their employment. That is, whether an employee's conduct may be prosecuted depends not on his or her action or intent, but on his or her job description. This exemption should alert all employers to the importance not only of specific job descriptions but also to clearly defined restrictions on each employee's computer access. By documenting and communicating the limits of employees' computer access, the employer reduces the risk of **unauthorized** entry and strengthens its position in potential civil or criminal litigation. Clear definition of employee computer access is thus essential.

The protections of the criminal justice system should be secondary to commonsense deterrent measures by employers. Prosecution for computer crime remains infrequent. Given the lack of technological sophistication in law enforcement and the difficulty of detecting computer crimes, employers should not rely on criminal laws as protection from computer abuse by employees. Because a public prosecution may disclose confidential data or highlight the lack of security in a system, criminal prosecution may be an undesirable way to deal with employee computer crime.

However, awareness of the problems that have prompted action by courts and legislators may help employers considering measures to prevent the various kinds of computer crime. For example, system software and stored data should be backed up and archived to ensure the prompt ability to recreate data damaged or erased by a disgruntled employee.

To prevent data destruction or theft, employers should plan carefully when they discharge computer knowledgeable employees or employees with access to company computer systems. Employees with significant computer access may be given pay in lieu of notice. Having the employee leave the premises as soon as possible could prevent computer abuse. Or, anticipating the discharge, the employer may block or change system passwords for on premises and remote use, thus eliminating that employee's ability to obtain or destroy data.

Written policies and procedures should address computer security issues. At a minimum, policies should define **authorized** access to specific systems and data. termination policies should include a provision for automatic discharge for the accessing of data beyond the employee's **authorized** level. Because **unauthorized** access is the conduct most widely prohibited by state statutes, a clear policy could facilitate the prosecution of a system intruder. More importantly, such policies should help deter tampering and similar misconduct.

Employer policies should also control copying and removing **stored** data. A balance must be struck between **protecting** against pirated **data** while still allowing for employee transportation of data to a home computer or other off-premises location for work needs. Some employers require supervisory approval before any data are removed from company premises, supplemented by logs showing which information has been removed, by whom, and when. Additional restrictions may be imposed to control removal of certain categories of data. Policies also should prohibit **unauthorized** copying by employees of licensed software to eliminate possible claims for royalties by software authors. Such claims may be lodged against the employer as wen as employees.

Security policies should emphasize that leaks of computer-stored data tend to occur without criminal intent. Such data may be duplicated or obtained in so many ways-from hard copy, storage, or transmission that employee carelessness is often the primary threat. This may be addressed with traditional management techniques, primarily establishment and dissemination of policy, training, and discipline for noncompliance. Indeed, employer inaction in the face of known risks to the security of computer data could be construed as acquiescence in security breaches, making it more difficult to respond effectively to employee misconduct or to encroachments on intellectual property.

Lawful and Effective Investigations

Prudent employers make clear to all employees their expectations of ethical conduct, yet maintain security policies and procedures that anticipate employee wrongdoing. Employees should know to whom within the company suspicions of wrongdoing should be disclosed. Effective policies facilitate prompt communication to employer-designated individuals at each business unit. These designated recipients should be trained to obtain maximum information promptly in a noncoercive atmosphere. Given the increasing speed at which data may be created, altered, or destroyed, rapid response time is crucial.

Initial recipients of the report of suspected wrongdoing should immediately notify a previously established team representing the legal, security, internal audit, and human resource functions. The team should begin to collect "documents" (as broadly defined as are discovery requests in litigation) and take steps to ensure the preservation of all relevant data in files, systems, or individuals possession. Because few investigations may be completed from documentary evidence alone, the team should also develop a strategy for interrogation and surveillance.

Important legal issues with respect to investigations should be considered from the outset. For example, even inan outside lawyer conducts the investigation, the related document or report may not be protected from disclosure. In Spectrum System International Corp. v. Chemical Bank, 1990 N.Y. App. Div. LEXIS 6972 (1st Dept. June 7, 1990), an internal investigation by a law firm regarding possible employee-vendor dishonesty was not covered by the attorney-client privilege because the work was not done in the firm's capacity as lawyers-not primarily for legal advice or services or anticipation of litigation-hence was not protected as attorney work product.

Employee interrogations in union settings

Whether security measures are enforced in a union or nonunion setting may determine how employees are interviewed. Whatever the setting, the investigatory interrogation should always be conducted in a noncoercive atmosphere and avoid any appearance of employer impropriety. Employers must also anticipate possible unfair labor practice charges under the National Labor Relations Act (NLRA) for not honoring an employee request to have a union representative or coworker present at the interview. In NLRB v. J.

Weingarten Inc., 420 U.S. 251 (1975), the Supreme Court held that an employee has a statutory right to refuse to submit to employer interrogation without union representation if the employee reasonably believes it will result in disciplinary action. As a corollary, the employer may not discipline or discharge the employee for refusal to cooperate without union representation.

Strict adherence to the Weingarten rule in union settings is recommended. This does not, however, prevent the employer from countering the employee's request for representation by offering the option of either an interview with no representation or the employer's continuation of the investigation without the interview. Weingarten has other limits: The statutory right of representation extends only to "employees" as defined by the NLRA, which excludes, among others, supervisors. Although employees may request the presence of a representative, they may not insist on having a specific representative present if that person is unavailable. The terms of the collective bargaining agreement also may define the process of selecting the representive who is to be present at interrogations. In those instances, the terms of the agreement would control any requests.

The Weingarten right of representation was for a time expanded by the National Labor Relations Board (NLRB) to include interrogation of nonunion workers. In Materials Research Corp., 262 NLRB 1010 data in files, systems, or individuals' (1982), the Board held that the right of concerted activity protected by the NLRA applies regardless of union status. The NTLRB then overruled Materials Research in Sears Roebuck and Co., 274 NLRB No. 55 (1985), holding that the language of NLRA "compels" the conclusion that Weingarten does not extend to nonunion employees.

After this absolute position was rejected in court,the NLRB overruled Sears Roebuck and was judicially affirmed when it concluded that Weingarten "should not" be extended to nonunion employees: In Slaughter v. National Labor Relations Board, 876 F.2d 11 (1989), the Third Circuit upheld the Board's finding that absent a collective bargaining representative, the employer (DuPont) could discipline a worker for refusing to discuss potential disciplinary matters without a representative of his choosing. Armed with the court's affirmance, the NLRB now has the discretion which it had sought to divest in Sears Roebuck. To date, the Board has made no additional decisions on nonunion employee interviews, so predictability is low.

The rapidly changing applicability of Weingarten to rights of nonunion, nonsupervisory employees the vast majority of those likely to be targeted for interrogation-suggests that careful legal advice should precede this phase of a security investigation. Weingarten continues to be an arena for the constant conflict between employees' due process rights and employers' responsibilities to protect confidentiality and workplace security.

Avoiding tort liability from employee interrogations The purpose of interrogating employees is to uncover evidence of misconduct or induce confessions. However, the method of interrogation may instead expose the employer to civil liability and create evidence that cannot be admitted in subsequent disciplinary or criminal actions. Improper interrogation typically creates claims of false imprisonment and defamation. The elements of these causes of action suggest what not to do when questioning employees.

False imprisonment occurs if an employer willfully detains the employee without his or her consent and without **authority** of law. The claim may arise from the mere "appearance of confinement" during questioning, which consists of the employee's reasonable belief that injury to person, reputation, or property would occur if he or she did not stay for the interview. False imprisonment may occur when a plaintiff gives up his or her freedom to leave an interrogation if the alternative is harm to his or her reputation; that is, if leaving would appear to confirm the allegations of impropriety. This often occurs when suspected shoplifters are detained in plain view of others.

Court decisions thus far hold that to detain an employee under threat of job loss is by itself insufficient to constitute false imprisonment. The theory is that an at-will employee, having no "right" to that job, gives up

nothing by leaving an interrogation and is therefore free" to move about voluntarily.[12] However, when an employee's personal reputation is also at stake, it is likely that involuntary restraint would be found if that were the perceived cost of leaving an interrogation.

Whether detention of an employee is deemed involuntary may depend on the duration of the questioning; increased duration increases the probability that it was involuntary. Even if the employer has good reason to believe that the employee was guilty of misconduct, a false imprisonment claim may still succeed if the confinement or detention was unreasonable under the circumstances. The burden to prove reasonableness of the confinement-including its duration and manner-is not on the plaintiff but on the employer.[13] Thus, regardless of the degree of employer suspicion, false imprisonment may still be found when force or its threat is used to detain the employee.

These elements of a false imprisonment claim suggest that employers that wish to use interrogation do the following: (1) ask the employee's consent to answer questions, (2) do not use physical force or its threat to detain a reluctant employee, (3) emphasize that the employee may leave at any time during the questioning, (4) limit the duration of the questioning to the time necessary to discuss the relevant matters, and (5) have a witness present.

Despite risks of false imprisonment claims, employers retain the right to expect cooperation in asking employees to reply to reasonable questions. Employees suspected of misconduct certainly may be confronted with the evidence and asked to explain, and witnesses may be interrogated. However, whether the employer acted reasonably may be a judicial issue. That a jury may be the ultimate arbiter should be a consideration in the employer's analysis of whether interrogation is necessary to the investigation. Can the employer obtain the same evidence without undertaking the risks of interrogation? May some form of disciplinary action be taken without confrontation?

Typical investigations do not invite a substantial risk of false imprisonment claims. Indeed, employees fired for misconduct without the opportunity to confront the evidence or their accusers probably pose more of a litigation threat than employees who must endure an interrogation. The employer's investigation team must weigh these risks prior to targeting candidates for interrogation.

The entire investigation process can expose the employer to defamation claims, a growth area in employment law. Although state laws on defamation govern the precise scope of protections and obligations, the employer's best defense in all jurisdictions is the qualified privilege." This privilege is not comprehensive because the central issues of truth and malice underlying its retention may still be decided by a jury. It is thus crucial that the employer's investigators understand the elements of the defamation cause of action as guidance to proper conduct.

A successful defamation claim requires proof that the employer made an untrue statement injurious to the employee's character. Security-related communications, usually involving issues of integrity, are almost by definition major influences on a person's reputation. The statement may be oral, written, or in the form of action. The existence of the qualified privilege is recognition of the public policy favoring frank exchange of information in hiring and evaluating employees. However, the privilege may be lost if the employee can show its abuse.

Three major factors determine whether an employer has abused its qualified privilege. The prudent employer will ensure that none occur. First, scrutiny of investigations for defamatory content increases with the seriousness of the alleged misconduct. As the potential increases for injury to character, so should the employer's degree of care increase as to the content of statements published about the employee. By labeling someone a criminal without compelling proof, in court the employer is likely to lose the qualified privilege. Or, by publishing allegations of serious misconduct-which could be tantamount to capital punishment for the employee's career-the employer may need more than a reasonable basis in fact to avoid a finding of abuse of privilege. Even truthful statements made with malice, particularly if they cast the employee in a false light,

can leave the qualified privilege in extreme jeopardy before a jury.

A second factor for employer consideration is the extent to which possible defamatory statements are published. Although state laws vary, publication has been held to include dictation to stenographers, personnel action taken in front of other employees, and release of information contained in an employee's personnel file. If a judge or jury determines that publication went beyond those people with a need to know about the alleged misconduct, the employer's qualified privilege may be lost. Preventive law dictates that employers should establish which individuals have a need to know based on their job responsibilities. Clear delineations of responsibility for security investigations should be included in written job descriptions to eliminate any question about need to know. The typical investigation of employee wrongdoing includes a team from among at least those line managers directly responsible, security, audit, and human resources staffers, and lawyers. This group, if not too large, would presumably have a need to know sufficient to avoid a trial on the issue.

A third factor is the relevance that the statements bear to the employer-employee relationship. Employers should avoid publishing statements about an employee's personal affairs that are not job-related or relevant to the investigation. Such communication could be deemed beyond the employment relationship and therefore outside the scope of qualified privilege. Not only would nonjob-related statements be subject to strict liability for any inaccuracies, they could also evidence abuse of the privilege that otherwise protects job-related statements.

A gray area exists when the employer seeks to communicate about the employee's capacity to work by describing family life or drug use. Even putting aside the likelihood of employment discrimination, such statements are unduly risky. Investigations of employee misconduct may suggest broader areas of inquiry that reach into personal life and proclivities and under some circumstances, these probes may be relevant. However, before expanding an investigation or making statements that appear to go beyond the employer-employee relationship, as traditionally understood (the standard applied by a jury), the prudent employer should obtain legal advice.

Notice and Reasonableness: Prerequisites for Surveillance

A rule of reason underlies successful security programs. Just as employees must be on notice of what constitutes unacceptable conduct, so must the employer take reasonable steps prior to instituting surveillance and searches. Absent sufficient preparation, employers inadvertently may expose themselves to arbitration, lawsuits, and work force demoralization. Even with proper preparation, measures that are responsive to identified needs are preferable to generalized surveillance. Because the triggering misconduct may be criminal or justify severe discipline, employers frequently held to rigorous due process requirements to support the personnel action and even the admissibility of the obtained evidence.

Employee expectations of privacy are paramount. Numerous arbitration and court decisions have depended on whether the employee was on notice that searches, pat-downs, or various kinds of surveillance would be undertaken. Decisions often turn on actual or implied notice and whether the employer acted reasonably in light of all the circumstances.[14] The lesson to be derived from case law is that employers should not rely on any third party's presumption about rights and responsibilities. Rather, employers should publish and disseminate policies of sufficient specificity that anyone will have a clear picture, from the employer's perspective, of workplace standards and employee understanding.

Given the myriad circumstances and techniques of employee surveillance, some general principles are useful. First, a sense of proportion is paramount: Is the surveillance reasonably necessary under the particular circumstances? Is the employee's right to privacy invaded to an extent not commensurate with the perceived threat?

Second, the purpose of the surveillance may dictate the legal consequence of each method: Generalized searches may be accorded less deference by courts or arbitrators than reasonable-cause searches supported by evidence of misconduct.

Third, gradations of privacy interests and expectations are afforded varying degrees of protection: Locker searches when the employer is known

to hold the master key stand up better than breaking employee locks, and searches with some precedent or with notice are more supportable than surprise sweeps.

Fourth, how personal the search dictates how much the law may protect the employee and punish the employer: Pat-down searches win get closer scrutiny than metal detectors, and closed-circuit television focused on the shop floor will get better judicial reception than one in the restroom. Similarly, surveillance of employees' off-premises, personal conduct raises such substantial risks to the employer that careful legal opinion should precede any such undertaking.

Fifth, constitutional and statutory protections of employee privacy rights must be understood and complied with: In O'Conner v. Ortega, 480 U.S. 714 (1987), government employees were held to be entitled to reasonable expectations of work-place privacy. Even though for purposes of the U.S. Constitution the prerequisite state action will not normally be imputed to nongovernment employers,[15] some states have enacted comprehensive privacy protections that do not require state action.[16]

Balanced against the legal risks of surveillance are valid business purposes that go beyond detection of employee misconduct. Employers have long monitored job performance to improve efficiency and control quality. Surveillance helps uncover workplace safety and health problems. Employers substantially at risk to theft or disclosure may strike the balance at the maximum amount of surveillance that is legally permissible-including the fun arsenal of technological devices and searches of office, desk, locker, or person. Such employers have to depend on clear policies that may include written consent of employees to undergo this extensive surveillance. Putting aside the likely effect on morale and productivity, these rigorous security programs portend substantial litigation and movements for legislation.

Fruits of off-premises surveillance of nonwork conduct often provide insufficient grounds for disciplinary action. Employer surveillance outside the employer-employee relationship may also divert otherwise arbitrable issues into jury trials. Off-premises, off-duty behavior may nevertheless be grounds for discipline if it (1) harms the company's reputation or product, (2) relates to the employee's inability to perform or appear at work, or (3) leads to refusal, reluctance or inability of other employees to work with the employee involved in non-work misconduct. These circumstances usually involve acts of moral turpitude, inherently subjective. Employers should avoid overreaction to nonwork behavior such as violent acts of self-defense or isolated use or possession of controlled substances. Advice of counsel should precede employer action.

Avoiding Claims of Malicious Prosecution

Even if surveillance reveals what the employer believes is criminal conduct by an employee, serious risk analysis should precede commencing with prosecution. Employer liability formalicious prosecution may occur if acquittal results and the employee can convince a jury that improper motive or malice motivated its initiation. Although probable cause to believe that the employee was guilty should refute claims of improper motive, results before a jury are unpredictable. For example, in Glover v. Fleming, 373 A.2d 981 (Md. Ct. Ap. 1977), an employer was found to lack probable cause by acting on an eyewitness report of the theft. At trial, the eyewitness was deemed to be untrustworthy.

Because of this unpredictability, employers should be wary about initiating prosecution themselves. Two safer approaches may help bring the employee to justice without undue employer risk:[17] First, the employer could turn all the evidence over to public **authorities** and let them decide whether to prosecute. This would in most cases shield the employer from successful claims of malicious prosecution. However, the employer must turn over all available evidence-exculpating as well-in order to avoid exposure. Second, rather than initiating prosecution, the employer could seek its attorney's determination of probable cause to prosecute. Attorney intervention may shield the employer from malicious prosecution charges, as long as the employer has made full disclosure. In both instances, the employer shows probable cause to believe in the employee's guilt and absence of malice in raising it with public **authorities** . Conclusion

Employers risk substantial liability from employee claims of victimization by workplace security programs. Preventive maintenance begins with written policies, adequately published and evenly enforced. Proportionality and reasonableness of security measures should further reduce these risks. Thus, traditional and sound personnel practices win enable workplace security programs to operate without undue risk to the employer.

NOTES

1. Black's Law Dictionary, 5th Ed. (1979)

2. States that have adopted the Uniform Trade Secrets Act: Alabama, Alaska, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Hawaii, Ilinois, Indiana, Kansas, Louisiana, Maine, Maryland, Minnesota, Montana, Nevada, New Hampshire, New Mexico, North Dakota, Oklahoma, Oregon, Rhode Island, South Dakota, Utah, Virginia, Washington, West Virginia, Wisconsin.

3. Maxwell, "Keeping the Secrets in Trade Secrets," Security Management 39 (1989).

4.Motorola. Inc. v. Contputer Displays Int'l., Inc., 739 F.2d 1149 (7th Cir. 1984);Structural

Dynamics Research Corp. v. Engineering Mechanics Research Corp., 401 F. Supp. 1102 (E.D. Mich. 1975).

5. "Computer Intruder Is Put on Probation and fined $10,000," N.Y. times, May 5, 1990, at 1, col. 1. The Computer Fraud and Abuse Act of 1986 applies only to **unauthorized** access to (1) government computers to obtain national defense or foreign relations information, (2) private industry computers of a financial institution, (3) computers operating in two or more states, or (4) "federal interest computers." and to interstate trafficking in computer passwords.

6. See, Gemignani What Is Computer Crime and should we care?," 10 U. Ark.Little Rock LJ. 55 (1988); Reimer, Judicial and Legislative Responses to Computer Crimes," 52 Ins. Couns. J. 406 (1986).

7. CCH, Guide to Computer Law, l 9920 Table) (April 12, 1990) citing the five states which outlaw viruses" as California, Illinois, Maine, Minnesota, and Texas).

8. Hancock v. Texas, 402 S.W .2d 906 (Tex. 1986); Ward v. Superior Court cited on p. 221).

9. National Sur. Corp. v. Applied Sys., So.2d 847 (Ala. 1982);People v. Weg, 450 N.Y.s.2d 957 (N.Y. Crim. 1982); U.S. v. David E. Kelly, 507 S. Supp. 495 (E.D. Pa. 1981). See generally, "Computer Crime Statutes: Are They Bridging the Gap between Law and Technology?," 11 Crim. Just. J. 203 (1988).

10. Guide to computer law cited in note 7).

11. Cal. Penal Code [section]502.

12. Foley v. Polaroid Corp., 400 Mass. 82, 508 N.E.2d 72 (1987); Columbia Sussex Corp. v. Hay, 627 S.W.2 d 270, 277-278 (Ky. 1981); Faniel v. Chesapeak & Potomac Tel. Co., 404 A.2 d 147,152 (D.C. Ct App. 1979); Moen v. Las Vegas Int'l Hotel, Inc., 90 Nev. 176.177 (1974).

13. See Foley v. Polaroid Corp. (cited in note 12).

14. See, Garbutt and Stallworth, "Theft in the Workplace: An Arbitrator's Perspective on Employee Discipline," 44 Arb. L. J. 21 (1989).

15. But see holodnak v. Avco Lycondng Div., 514 F.2d 285 (2d Cir.), cert denied, 423 U.S. 892 (1975) First Amendment applicable to employees of government contractor).

16. See, e.g., California Constitution, Article 1. Section I, and Cal. civ. Code [section]1798.53.

17. See, Gowin v. Altmiller, 455 F. Supp. 743 (D. Idaho 1978), aff'd 647 F.2d 170 (9th Cir. 1981).

INDUSTRY CODES/NAMES: INSR Insurance and Human Resources; GOVT Government and Law; BUS Business, General

DESCRIPTORS: Industry--Safety and security measures; Employees--Laws, regulations, etc.

GEOGRAPHIC CODES: NNUS

FILE SEGMENT: LRI File 150

?

? t s9/full/7

9/9/7 (Item 1 from file: 275)

01319939 SUPPLIER NUMBER: 08042740 (THIS IS THE FULL TEXT)
Does your DP department bear investigation? (data processing)
Finn, Tony
DEC User, p56(2)
Dec, 1989
ISSN: 0263-6530 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 2187 LINE COUNT: 00159

ABSTRACT: This first of two articles describes how to prevent **unauthorized** physical access to a data processing (DP) department. The very basic security measures should include having people sign in as they enter, barring visitors **without permission** , letting DP management know when visitors are in, and requiring all visitors to wear identification badges. Added measures should include alarms on doors that are left open, special procedures for disposing of unwanted tapes and disks, and a private way of throwing away discarded printouts. Back-up tapes or disks of all data should be stored in a secure place that neither fire, thieves, or acts of God can reach.

TEXT:

Does your DP department bear investigation? TODAY IS one of the few days in the year when you walk with a spring in your step. You've just returned from your annual two weeks in the sun, today is your first day back at work and all is right with the world. At the top of the pile in your in-trayis the status report from your systems manager. He starts his three weeks' holiday today, but there are few problems outstanding and you have a contract systems manager to cover in his absence. You put the report to one side to answer the phone. It's your boss's secretary: can you come up and see CJ straight away?

Ah, John ... nice holiday? good ... good,' he says. 'I'd like you to meet Mike Nerd from Coopers, Andersen, McClintock, Freeman, Hardy and Gorbachev, our auditors.' You shake the proffered hand, dimly wondering why this man is here. 'Mike is here to do the DP audit I told you about before you went on holiday,' continues CJ, 'so I'll leave him in your capable hands.'

What DP audit? Now you have got to release this super-sleuth on your department while your systems manager, the only one who knows where the bodies are buried, is away.

Those of you who can identify with this situation read on.

THE AUDITORS. The role of the DP auditor has changed considerably since the early 1970s. In those days it was common practice for one of the accountants from the general accounts audit, usually the one with a little bit of computer awareness, to pay a quick visit to the DP department to check out a few things. This usually took a day and consisted of checking the payroll records of the computer staff for any discrepancies and maybe a check on the orders for consumables. The DP audit was then complete!

As DP activities in client sites broadened and DP departments began to provide services outside the accounts and payroll departments, management consultancy and chartered accounting firms developed new skills to enable them to undertake a detailed audit of the DP functions.

As well as providing generic courses on DP auditing as part of their internal training facilities, many of the large auditing companies send their DP audit staff on courses to acquaint them with the technical aspects and security features of systems such as Vax/VMS, AS400/OS400 and System 38.

The chances are that when your DP auditor turns up, he or she has already attended a Vax/VMS security seminar, is a member of the EDP Auditors Association and knows more than a little about the workings of

VMS. When dealing with your auditor, it pays not to underestimate him or her.

It is worth remembering that the auditor is acting for the shareholders in validating that your company's data and processing equipment is protected, secure and well managed. If you are an IT professional worth your salt, these aims will also be yours.

PHYSICAL ACCESS SECURITY. Physical access security starts at the front door of the building and sets the level of expectation on what is to come as one proceeds throughout the building. A company with a policy of signing visitors in and out, issuing them with temporary visitors' passes, and accompanying them during their visit is much more likely to inspire confidence than one where visitors are passed through because everyone is too busy to keep an eye on them.

Although the overall building security may not appear to be an IT concern at first glance, a sloppy security policy can have a major impact on you and your users. I know several organisations where maintenance engineers turn up unannounced at user sites, are ushered in like returning prodigals and allowed unrestricted access to systems and communications facilities. Many City-based DP staff have a supply of war stories about the day that the dealing room lost all its data feeds because an engineer came in and took the system down 'just for a few minutes' without telling anyone.

At the very least, the IT department should be satisfied that:

* Receptionists sign people in;
* No visitors are allowed access to IT rooms **without permission** ;
* Visitors to IT areas are announced to IT management;
* All visitors are issued with visitors' badges and told to wear them.

Of course, even these few basic procedures leave an awful lot to chance; so what more can be done? To begin with, areas containing IT equipment such as the PABX room, communications/computer room and so on should have keycard access. Keycard systems can come as expensive as you like, with very impressive 'hands off' systems at the top end of the scale. A basic keycard system with a Pin number on the card unique to each user should be more than adequate in the majority of sites, as long as the card distribution is restricted to those who need access to the protected areas, and there are no visitors' keycards in reception.

Without exception, visitors to protected rooms should be accompanied by a member of staff **authorised** to access the protected area and should never be given their own keycard for access purposes. Keycards should be reissued periodically, and there should be a procedure to withdraw the cards when a member of staff leaves the organisation. Finally, visitors should be logged in and out of restricted areas, even though they are accompanied.

So now we have a degree of protection against **unauthorised** access and that should gain us some brownie points with the auditor. What next?

Have you ever come in early in the morning, just before the night shift goes home, to see how well security procedures are observed? To begin with, don't be too surprised to find that the doors with keycard access are jammed open to ease the movement of boxes of reports out of the computer operations area. You may even find that you can walk in from the street through to the operations area without encountering a single locked door. The usual reaction from operations to your complaint about this state of affairs will be that 'It's too early for anyone to be about, and it will all be back to normal by 8 am'.

The solution to this problem is to fit alarms to each restricted access door and wire the alarms through to the reception area in the building. Each time a door is jammed or held open for more than a set time, the alarm goes off. The receptionist/security person gets sick of the noise and words are exchanged between security and operations. The problem soon goes away.

What happens to your old magnetic tapes, floppy discs and removable disc packs when they reach the end of their useful life? Are they demagnetised/shredded/smashed before being put in the bin, or are they just thrown out with the rest of the rubbish?

No auditor likes to see a tape or disc labelled 'Meglamania Ltd Profit & Loss Report, Q2 1989' hanging out of a bin bag outside the back door of the building, even if the media has been demagnetised. It pays to make periodic checks that media and confidential data are being disposed of correctly. It is also worth considering the employment of a confidential waste disposal company to remove your secure rubbish and dispose of it properly.

Another area to be investigated is the disposal of printed output by user departments. It is a fact of life that a percentage of all printed output is filed under WPB (waste paper bin) without ever being read by the recipient. A further percentage of reports is dumped within a week of receipt and only a small percentage is filed away for reference purposes. This means that a large amount of the company's data is dumped in bins along with Mars bar wrappers and empty cigarette packets, while it is still current, providing the competition with untold opportunities to access this data and use it to build up a picture of the company's activities.

This may sound a bit fanciful, but before you dismiss the possibility, consider the fact that in the UK today there is a fast growing market in electronic surveillance and electronic eavesdropping equipment. If people are prepared to use these devices to spy on the competition, how do you know that your competitor doesn't pay one of your office cleaners to collect reports every day and pass them on?

Once again the use of a confidential waste disposal company will reduce the risk of secure waste falling into the wrong hands. It is sensible to place special secure waste bins in each department and to encourage the department managers to use this method to dispose of confidential reports.

Microfiche has grown in popularity for storing reports, and the disposal of microfiche needs to be looked at carefully along with the disposal of printed reports. Disposal via a confidential waste disposal company would again appear to be the safest route.

Many people would argue that the security and disposal of old magnetic media, reports and microfiche is the responsibility of office services, and not the IT department. I would suggest that it's a joint responsibility, especially when one considers that IT staff know better than most how sensitive the information on the media or in the reports is.

It may also seem poetic licence to deal with these items under the heading 'physical access security', but surely the act of taking away media or printed reports is 'physical' access?

If your site already has adequate procedures to deal with the problems outlined so far, the chances are that your auditor loves coming to your site, and for you God is in His heaven and all is right with the world. For most of us, this state of Nirvana is always aimed for but never achieved. Don't despair -- at least, not yet.

BACKUP STORAGE. Most sites make regular backups of their disc storage, but not all sites put the backups off-site. For our purposes, off-site means in a different building to the primary storage media, not necessarily 50 miles away in a bomb-proof bunker.

Many users feel that it is sufficient to put the backup tapes in a fire-proof safe in a corner of the computer room to give all the protection they need. I will relate a cautionary tale especially for these people and let them draw their own conclusions.

Some years ago, a businessman in Belfast decided to invest in a fire-proof safe for his backup tapes. He purchased a quality safe with all the latest features, and installed it in the corner of his computer room on the third floor of his building. One night, a car bomb went off outside the building, and the building was badly damaged by fire as well as by the impact of the blast. The next morning, the businessman was shocked to see the extent of the damage, but offered a silent prayer of thanks that he had invested in a fire-proof safe.

However, the police refused to allow him access to the safe, which had fallen from the third to the ground floor but was still intact, because the whole building was unstable. By the time the building was stable enough for the businessman to be allowed near his safe, five days had passed and he had gone out of business. When he opened the safe, all the tapes were in

good condition, and had survived the safe's fall as well as the explosion and the fire.

A number of specialist 'storage firms will collect your off-site storage material from your site and store it in a controlled air-conditioned environment for you. Typically they will deliver it back to you within an agreed time, any time, day or night. For this level of peace of mind, you will pay a fee.

Those of you who don't need this type of service can consider a reciprocal arrangement with another user, or can store the backup media at another of your company's offices, or you can put the backup media in the vault of your local bank. In short, there are any number of means available to you to satisfy your off-site storage requirements. The important point is that you realise that a fire-proof safe on its own is not enough to **protect** your corporate **data** , and that is what your auditor will be concerned with.

DESCRIPTORS: Data Processing; Auditing of Computer Systems; Data Security ; Tutorial
FILE SEGMENT: CD File 275
?